PROYECTO FIN DE MÁSTER EN

SISTEMAS INTELIGENTES

CURSO 2011-2012

MECANISMO DE SEGURIDAD PARA REDES MÓVILES HETEROGÉNEAS

Ismail Saadat

Director:

Luis Javier García Villalba

Departamento de Ingeniería del Software e Inteligencia Artificial

---

MÁSTER EN INVESTIGACIÓN EN INFORMÁTICA

FACULTAD DE INFORMÁTICA

UNIVERSIDAD COMPLUTENSE DE MADRID

El abajo firmante, matriculada en el Máster en Investigación en Informática de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: "***Mecanismo de Seguridad para Redes Móviles Heterogéneas***", realizado durante el curso académico 2011-2012 bajo la dirección de Luis Javier García Villalba en el Departamento de Ingeniería del Software e Inteligencia Artificial, y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.

_____

Ismail Saadat

Abstract

The current Thesis concentrates on the design of a security mechanism for handovers in next generation networks giving the mobile user the necessary functionality that will allow him or her to move between the multiple access networks (like Wi-Fi, Wi-Max and 3G) in a transparent and secure manner, this way enjoying IP communication from any place and at any moment. In the next-generation networks, mobile users can use an information server that stores information from neighbouring networks in order to reduce the processing and overhead in the network discovery process. Communication between the user and the information server must be completely safe. Therefore, the main goal of this Thesis is specifying a security mechanism for handovers using a hierarchical framework of network information servers, considering neighbourhoods with multiple operators offering relevant information so that the mobile user can make a correct transition without any human intervention, based on the characteristics of the user and the networks resources, improving undoubtedly the handovers quality.

Keywords

IEEE 802.21, information server, hierarchical MIIS, heterogeneous networks, MIH, security.

Resumen

La presente tesis se concentra en el diseño de un mecanismo de seguridad para transiciones en redes de nueva generación proporcionando al usuario móvil las funcionalidades necesarias que le permitan itinerar entre múltiples redes de acceso (como Wi-Fi, Wi-Max y 3G) de forma transparente y segura, disfrutando así de comunicación IP en cualquier lugar y en todo momento. En las redes de nueva generación el usuario móvil podrá utilizar algún servidor de red que almacene información de sus redes vecinas con el objetivo de disminuir el procesamiento y la sobrecarga en el proceso de descubrimiento de redes. La comunicación entre el usuario y el servidor de información debe ser totalmente segura. Así, el principal objetivo de esta tesis es especificar un mecanismo de seguridad para transiciones mediante la utilización de una arquitectura jerárquica de servidores de información de red, considerando entornos con múltiples operadores que ofrezcan información relevante para que el usuario móvil haga una transición correcta y sin ninguna intervención humana, basándose en las características del usuario y los recursos de las redes, lo que mejorará indiscutiblemente la calidad de las transiciones.

Palabras clave

IEEE 802.21, servidor de información, MIIS jerárquico, redes heterogéneas, MIH, seguridad.

Agradecimientos

Primero, y antes que nada, doy gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio. Agradezco también hoy y siempre a mi familia porque a pesar de no estar presentes físicamente, procuran mi bienestar desde mi país, Palestina, y si no fuese por el esfuerzo realizado por ellos mis estudios de máster no hubiesen sido posible.

Segundo. Me gustaría agradecer a mi esposa y a mis hijas que habéis compartido conmigo uno de los momentos más difíciles de mi vida. Por el amor, cariño y por la fuerza que me habéis dado, os agradezco de corazón y os quiero (y querré siempre).

Tercero. Agradezco a Javier García por haberme dirigido y acompañado durante todo el proyecto.

A mis compañeros del Grupo de Análisis, Seguridad y Sistemas (GASS) que me ha dado ofrecido su apoyo y al Departamento de Ingeniería del Software e Inteligencia Artificial (DISIA) de la Facultad de Informática.

Finalmente, agradezco a todas personas que de una u otra forma me han ayudado.

Lista de acrónimos

3G	Third Generation Networks
3GPP	Third Generation Partnership Project
4G	Fourth Generation Networks
AAA	Authentication, Authorization and Accounting
AP	Access Point
API	Application Programming Interface
BSS	Basis Service Set
CDMA	Code Division Multiple Access
CIP	Cellular IP
CoA	Care-of Address
CPS	Common Part Sublayer
CS	Convergente Sublayer
DAD	Duplicate Address Detection
DAIDALOS	Designing Advanced network Interfaces for the Delivery and Administration of Location Independent, Optimised Personal Services
DHCP	Dynamic Host Configuration Protocol
EDGE	Enhanced Data Rates for Global Evolution
ESS	Extended Service Set
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HA	Home Agent
HMIPv6	Hierarquical MIPv6

HoA	Home Agent
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Eletronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Networks
LLC	Logical Link Control
MAC	Médium Access Control
MAN	Metropolitan Area Networks
MIB	Management Information Base
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIHO	Mobile Initiated Handovers
MIIS	Media Independent Information Service
MIP	Mobility IP
MIPv6	Mobility IP version 6
MLME	MAC Layer Management Entity
MN	Mobile Node
NAT	Network Address Translation
NIHO	Network Initiated Handovers

pCoA	Proxy Care-of Address
pHoA	Proxy Home Address
PHY	Physical Layer
PLME	Physical Layer Management Entity
PMIPv6	Proxy Mobile IPv6
PoA	Point of Attachment
PoS	Point of Service
QoS	Quality of Service
RSS	Radio Signal Strength
RSSI	Radio Signal Strength Indication
SAP	Service Access Point
SIP	Session Initiation Protocol
SSID	Service Set Identifier
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WEP	Wired Equivalent Privacy
Wi-Max	Worlwide Interoperability for Microwave Access
Wi-Fi	Wireless Fidelity (Wireless Local Area Network)
XML	eXtensive Markup Language

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

Usted está casi listo para lo que podría ser la reunión más importante del año en su compañía. Tiene en sus manos su comunicador personal mientras toma un taxi para encontrar a sus compañeros en una cafetería cercana antes de salir para el aeropuerto. Su comunicador es un teléfono móvil de última generación que tiene diversas interfaces de comunicación como GPS, Wi-Fi, 3G, Bluetooth, y banda ancha inalámbrica Wi-Max.

A medida que se acerca a una cafetería, la capacidad de movilidad inteligente de su comunicador detecta un *hotspot* Wi-Fi y acciona la interfaz WLAN. Mientras se reúne con sus compañeros de trabajo empieza a descargar un anexo de última hora para su presentación utilizando la red local inalámbrica Wi-Fi de la cafetería. Al mirar el reloj descubre que está atrasado. Mientras usted sale de la cafetería para tomar un taxi en dirección al aeropuerto pierde su conectividad Wi-Fi y su comunicador pasa su conexión a la red Wi-Max para mantener la operación de descarga en curso. Paralelamente, usted hace un par de llamadas rápidas utilizado la red celular 3G. En su camino hacia el aeropuerto, su comunicador le avisa que está con la batería baja y pasa a una conexión GPRS que consume menos energía cerrando la conexión Wi-Max. En el aeropuerto, usted conecta su comunicador a un enchufe y el comunicador se conecta por Wi-Fi una vez más, después de haber detectado un *hotspot* para completar la descarga del archivo.

Este escenario, que será real en muy poco tiempo (o ya lo es), incluye un dispositivo de comunicación personal con cinco interfaces de radio, obteniendo servicios de cuatro proveedores de red u operadores diferentes, con velocidad de transmisión de datos que van desde 7,2 Mbps para el servicio celular, 600 Mbps para las redes Wi-Fi en la cafetería y en el aeropuerto y hasta 1 Gbits/s

para la red de banda ancha Wi-Max. El escenario anterior dramatiza la premisa básica del estilo de vida móvil emergente: la conectividad siempre presente en cualquier lugar, en cualquier momento y utilizando las redes disponibles [Intel].

Cuando se habla de movilidad e interoperabilidad entre redes, el usuario espera que el retardo sea mínimo o ninguno y que todo sea realizado sin ninguna intervención humana. Para optimizar la transición entre los medios heterogéneos se creó el estándar IEEE 802.21 [802.21] a principios del año 2009. Este estándar se encarga de mejorar la experiencia del usuario y facilitar el intercambio entre distintas redes de comunicación, como son las redes 3GPP, 3GPP2 [3GPP] y las redes inalámbricas pertenecientes a la familia IEEE 802: Wi-Fi [802.11] y Wi-Max [802.16]. El estándar también es conocido como Transición Independiente del Medio (MIH).

El estándar proporciona una arquitectura de movilidad que permite gestionar la interconexión de distintas redes inalámbricas posibilitando una continuidad de servicio transparente mientras que un terminal móvil hace la conmutación entre las tecnologías. Como se muestra en la Figura 1.1, la arquitectura de movilidad consta de 3 niveles. En el nivel intermedio tenemos la Función de Transición Independiente del Medio (MIHF) que es el principal componente del estándar IEEE 802.21. El MIHF se encarga de gestionar la comunicación entre las capas inferiores y superiores. En el nivel superior están los usuarios MIH, que son aplicaciones o protocolos de movilidad (p.e. IP Móvil [MIP]) que utilizan la información ofrecida por el MIHF para la toma de decisiones de cuándo hacer la transición entre dos redes. Por último, el nivel inferior se refiere a información relativa a las capas físicas y capas de enlace, es decir, todos los cambios que ocurren en la interfaz se generan en este nivel y se envían al MIHF. De lo anterior, hay un conjunto de servicios que son necesarios para que haya comunicación entre las capas inferiores y las capas superiores de

la arquitectura de movilidad.

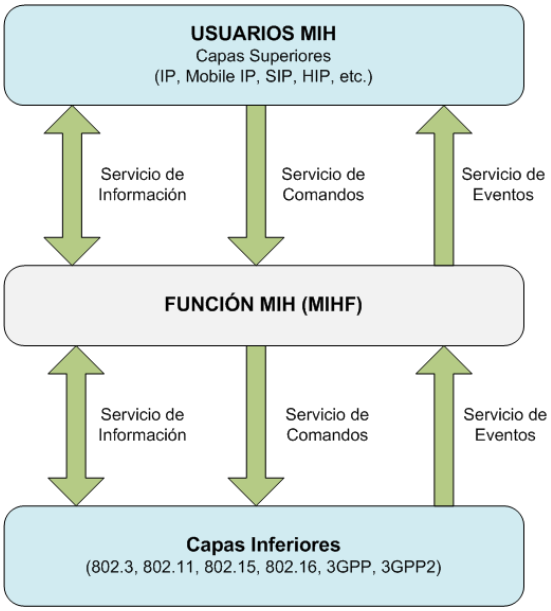

Figura 1.1: Arquitectura general del estándar IEEE 802.21.

La función MIH ofrece 3 tipos distintos de servicios. Estos servicios son:

a. **Servicio de Eventos (MIES)**: servicio que detecta cambios en las propiedades de las capas físicas y de enlace y dispara eventos que se envían a la función MIH. Estos eventos pueden generarse tanto en el MIH local como en MIH remotos. Un ejemplo de un servicio de evento es el nivel de recepción de la potencia de la señal por parte de un nodo móvil. Cuando la señal empieza a debilitarse, la capa de enlace envía un evento a la función MIH. Basándose en esta información, el usuario móvil cambia su conexión, conectándose a una red con mejor señal.

b. **Servicio de Comandos (MICS)**: servicio que permite a los usuarios MIH controlar, configurar y obtener información de las capas inferiores incluyendo la capa de enlace y la capa física. Como ejemplo se puede mencionar el comando *Link Get Parameters* que permite a los usuarios MIH descubrir información de la interfaz activa como relación señal ruido, tasa

de errores de datos, nivel de recepción de la señal, etc.

c. **Servicio de Información (MIIS)**: servicio que ofrece mecanismos que permiten a una función MIH descubrir y obtener información de las redes existentes dentro de un área geográfica. Se puede modelar el servicio de información como una base de datos que almacena información de las redes (tipo de red, frecuencia utilizada, seguridad, coste del servicio, velocidad de transmisión, configuraciones IP, etc.).

Un ejemplo de cómo de útil puede ser el estándar IEEE 802.21 en la movilidad de los usuarios, puede encontrarse cuando un usuario hace uso de la aplicación de VoIP Skype. En un determinado momento la interfaz de red (nivel inferior) detecta que la calidad de la señal está disminuyendo considerablemente notificándolo al MIHF. El MIHF comunica a la aplicación Skype (nivel superior) que toma la decisión de seguir en esta red y sufrir posiblemente una pérdida de información o bien decide cambiarse de red buscando una conexión que le proporcione una mejor calidad de comunicación.

Este capítulo tiene por objeto ubicar el presente trabajo de investigación. La sección 1.1 contiene motivación en el área de este trabajo. La sección 1.2 resume los principales trabajos existentes en el área. A continuación, la sección 1.3 delimita el tema presentando los objetivos de este trabajo. Finalmente, la sección 1.4 muestra la organización de los siguientes capítulos de esta memoria.

1.1. Motivación

La posibilidad de hacer transiciones de las conexiones de voz, de vídeo y de datos en cualquier momento y en cualquier lugar es muy atractivo para el usuario final. A medida que el nuevo estilo de vida móvil se hace más presente, los dispositivos de funciones fijas de red abren paso a dispositivos móviles

multifuncionales. Diariamente salen al mercado teléfonos 'Wi-Fi, GPS y 3G'. Este hecho unido a la promesa de un ancho de banda aún mayor y mejores experiencias de usuario dan impulso a la adopción de una Internet cada vez más inalámbrica.

En la Figura 1.2 se puede vislumbrar un esquema de cómo será (es) el nuevo entorno de comunicación de un usuario móvil donde redes de acceso Wi-Fi, Wi-Max y 3G pueden coexistir. En este ejemplo, un usuario móvil se mueve por un determinado área de la ciudad de Madrid, teniendo la posibilidad de conectarse a diferentes tipos de tecnologías inalámbricas pertenecientes a diferentes operadores. La elección de una red se basa en las preferencias del usuario. Así puede conectarse solamente a redes gratuitas, a las redes que ofrezcan un ancho de banda suficiente para que pueda seguir disfrutando de una aplicación música o de vídeo, etc.

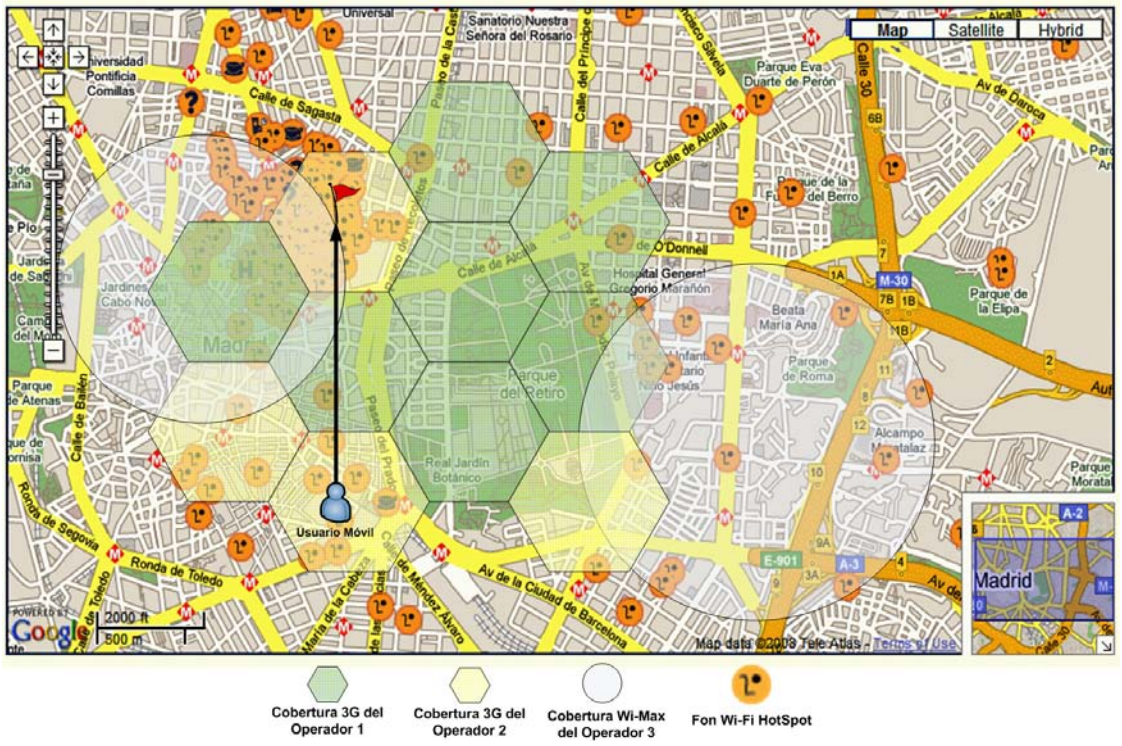

Figura 1.2: Escenario de movilidad entre redes heterogéneas.

La llegada de nuevos dispositivos móviles compatibles con múltiples radios proporciona grandes desafíos, particularmente en lo relativo a la movilidad. Los dispositivos deberán ser capaces de detectar y seleccionar automáticamente la mejor red inalámbrica y de proporcionar una transición transparente de una red a otra.

En redes celulares, la transición entre estaciones base es automática y el usuario apenas nota un retardo o pérdida de información en la conversación. El nivel de la señal normalmente es el parámetro por el cual el dispositivo móvil decide elegir una red u otra. En redes IP [RFC791], como las redes Wi-Fi y Wi-Max esta transición tiene mayor complejidad, ya que varios factores como calidad de servicio (QoS), seguridad, coste, tipo de red, configuraciones IP, prestaciones del terminal móvil, etc., influyen de forma considerable en la decisión de elegir la mejor red. Unir todas estas tecnologías con arquitecturas diferentes, algunas con protocolos e implementaciones propias, es un gran reto.

Para que un usuario móvil pueda utilizar todas las redes del escenario de la Figura 1.2 y disfrutar de una comunicación ininterrumpida durante todo su trayecto, debe realizar tres tareas: (1) descubrir las redes disponibles en una determinada zona geográfica; (2) elegir una de las redes de acuerdo con sus preferencias y (3) ejecutar la transición de una red a otra.

De las tres fases la tarea de descubrimiento de redes es la que más tiempo demanda por parte del usuario, ya que debe realizar un barrido de forma periódica en búsqueda de nuevas redes. Como se ha comentado anteriormente, el estándar ofrece un servicio de información (MIIS) donde el usuario puede obtener información sobre las redes en una determina zona, que estaría almacenada en un servidor central. Utilizando este servidor, un usuario conectado a una red Wi-Fi puede saber de la existencia de redes 3G o Wi-Max sin la necesidad de activar la interfaz de estas tecnologías, ahorrando tiempo y energía.

En la literatura, cuando se presenta el servidor de información, típicamente tiene las siguientes características:

a. El servidor está ubicado físicamente en algún lugar del backbone del operador.

b. El usuario o alguna entidad de la red envía un mensaje de solicitud de información al servidor, que responde al usuario móvil con información detallada de las redes de acceso disponibles.

De forma resumida, el estándar así como prácticamente la totalidad de los trabajos existentes (véase sección 1.2) consideran la existencia de un servidor de información que responde a las solicitudes de los usuarios con información de las redes disponibles. Estas propuestas son bastante limitadas en lo que se refiere a la arquitectura de servidores de información, a su funcionamiento y a la gestión de información de movilidad, sobre todo si consideramos escenarios heterogéneos y de gran escala. La cantidad de redes de acceso, operadores y usuarios móviles impactan directamente en el aprovisionamiento de información por parte del servidor, pudiendo afectar a la calidad de la información ofrecida al usuario, haciendo que el usuario tenga una visión errónea de las redes y los recursos disponibles. Asimismo, otro problema común a las propuestas existentes es la especificación de un solo servidor para gestionar toda la información de movilidad. La especificación de un único servidor de información de red presenta muchos inconvenientes:

a. **Demasiada información que almacenar** si existen cientos o miles de redes de acceso y decenas de operadores.

b. La existencia de **un único punto de fallo** en la red.

c. **Gran retardo** en recibir la información si el servidor MIIS está a muchos

saltos del usuario móvil.

d. **Elevada sobrecarga**, ya que cada solicitud de información del usuario tiene que llegar al servidor centralizado.

e. Poca o **ninguna escalabilidad** si hay muchas peticiones simultáneas en escenarios con gran número de usuarios.

Es evidente que el uso de un servidor de información para una ciudad o para un país con diferentes operadores no es lo más deseable. Puesto que si el servidor envía al usuario información errónea, realizará una transición incorrecta.

La motivación de este trabajo es, por tanto, la especificación de un sistema de información de movilidad, que informa al usuario móvil sobre las redes y los recursos disponibles en una determinada zona geográfica. Este sistema permitirá reducir el tiempo de descubrimiento de información de redes vecinas y mejorar la calidad de las transiciones entre redes de diferentes tecnologías y en ambientes con múltiples operadores.

1.2. Objetivos

El objetivo principal de este trabajo es especificar un mecanismo de seguridad para un sistema jerárquico de servidores de información MIIS que sea flexible y escalable.

1.3. Estructura de la Memoria

Este trabajo está organizado en seis capítulos, siendo el primero la presente introducción.

El capítulo 2 presenta el estándar IEEE 802.21, sus elementos, entidades y mensajes así como un detallado análisis de la fase de preparación de la transición (el descubrimiento de redes de acceso). También recoge un exhaustivo análisis del estado del arte de la tecnología IEEE 802.21.

El capítulo 3 describe la especificación de un sistema de información de movilidad que reduce el tiempo de descubrimiento de redes vecinas y mejora la calidad de los *handovers* entre redes de distintas tecnologías y con diferentes operadores. El sistema especificado considera la división de las redes de acceso en zonas geográficas de movilidad, clasificadas de forma jerárquica, y administradas por distintos tipos de servidores MIIS: MIIS Zonal, MIIS Local y MIIS Global.

El capítulo 4 hace un análisis de los principales mecanismos y protocolos de seguridad para redes móviles heterogéneas, haciendo énfasis en el protocolo MPA por ser el principal referente.

El capítulo 5 presenta la principal contribución de este trabajo: la especificación de un mecanismo de seguridad para un sistema jerárquico de servidores MIIS.

Finalmente, el capítulo 6 presenta las conclusiones obtenidas así como las orientaciones futuras que podrá tomar este trabajo.

2. EL ESTÁNDAR IEEE 802.21

Este capítulo está dedicado al nuevo estándar IEEE 802.21 que ofrece una arquitectura de movilidad que permite la interoperabilidad entre redes heterogéneas.

Se empieza con un repaso de los principales conceptos del estándar IEEE 802.21, también conocido como: "Transición Independiente del Medio" (abreviadamente MIH, Media Independent Handover), señalando sus objetivos, características y aplicaciones. También se describe la entidad principal del MIH, su modelo de referencia, sus características y sus principales servicios para soportar una transición entre redes heterogéneas.

Posteriormente, se muestra un ejemplo de una transición entre una red Wi-Fi y una red Wi-Max con especial énfasis en el intercambio de mensajes entre el usuario, los puntos de acceso de ambas redes y el servidor de información que almacena la información de todas las redes en la vecindad del usuario móvil.

El capítulo finaliza con una breve síntesis de lo expuesto en el mismo.

2.1. Introducción

El grupo de trabajo compuesto por más de 80 empresas tecnológicas (Nokia, Siemens, NEC Europe, InterDigital, T-System, NIST, Telcordia Technologies, Alcatel-Lucent, Intel, Motorola, etc.) y más de 300 investigadores pertenecientes a varios centros de investigación y desarrollo de todo el mundo, comenzó la especificación del estándar en marzo de 2004. Se elaboró un borrador en 2005 con la definición inicial del protocolo. En enero de 2009 se publicó la versión final del estándar.

El objetivo principal del estándar es mejorar la experiencia del usuario y facilitar la transición entre distintas redes de comunicación. Para ello el estándar proporciona una arquitectura de movilidad que permite gestionar la interconexión de distintas redes inalámbricas posibilitando una continuidad de servicio transparente mientras que un usuario móvil hace la transición entre diferentes tecnologías.

Como se muestra en la Figura 2.1, la arquitectura de movilidad consta de 3 niveles. En el nivel intermedio tenemos la Función Transición Independiente del Medio (abreviadamente MIHF, Media Independent Handover Function) que es el principal componente del estándar IEEE 802.21. El MIHF se encarga de gestionar la comunicación entre las capas inferiores y superiores. Las capas inferiores se refieren a las capas físicas y de enlace, es decir, todos los cambios que ocurren en la interfaz se generan en estas capas y se envían al MIHF, que se encarga de renviarlos a las capas superiores, también conocidos como Usuarios MIH (abreviadamente MIHU, MIH User). Estos pueden ser una aplicación o algún protocolo de movilidad. Asimismo, existe un conjunto de servicios que son necesarios para que haya comunicación entre las capas inferiores y las capas superiores de la arquitectura de movilidad.

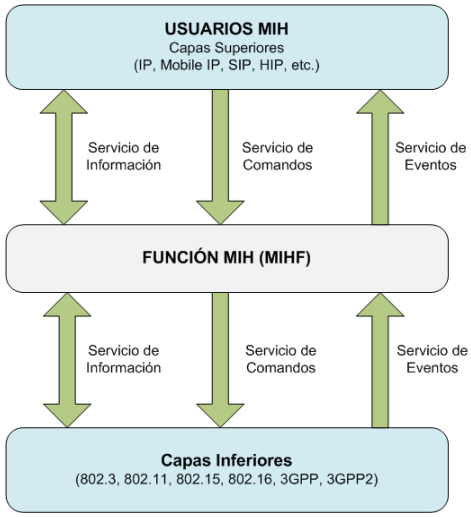

Figura 2.1: Arquitectura general del estándar IEEE 802.21.

El estándar soporta transiciones tanto para nodos móviles como para nodos fijos. Para los nodos móviles la transición puede ocurrir como consecuencia de cambios en las condiciones del enlace inalámbrico. Los nodos fijos pueden solicitar la transición cuando haya una red más atractiva que otra (en términos de ancho de banda, coste, QoS y seguridad).

La cooperación entre el usuario móvil y la red es de fundamental importancia para el funcionamiento del protocolo 802.21. El usuario debe detectar las redes que estén disponibles en su área de cobertura y la red debe almacenar la máxima cantidad de información de las redes vecinas. Información como la lista de los puntos de acceso en la vecindad, localización de los usuarios móviles y la disponibilidad de servicios de las capas superiores deben almacenarse en una entidad de la red, que puede ser centralizada o distribuida dependiendo de la cantidad de operadores y del tamaño de la red en cuanto a números de puntos de acceso, usuarios móviles, etc.

La decisión de hacer la transición la puede tomar el usuario móvil o la red a la que el usuario esté asociado. Basándose en la información contenida en un servidor de información, el usuario puede iniciar la transición de una red a otra. Por ello, el nodo móvil y la red deben soportar múltiples interfaces de comunicación como Wi-Fi, Wi-Max, UMTS, 3G, etc., además de permitir conexiones simultáneas en más de una interfaz.

Para ofrecer transición entre redes heterogéneas de forma transparente al usuario móvil, el estándar posee las funcionalidades que se indican en la Figura 2.2:

- Una arquitectura que permite a un usuario móvil moverse entre distintas redes (diferentes capas de enlace) sin pérdida de conectividad. La arquitectura cuenta con la presencia de una pila de protocolos de gestión de movilidad en cada elemento participante de la red, sea un terminal

móvil, un punto de acceso o un router.

- Un punto de conexión (MIH_SAP) entre el MIHF y los usuarios MIH, que son los protocolos de capa de red o superiores. La existencia de este enlace permite a los usuarios MIH acceder a la información de las redes antes de hacer la transición entre ellas.

- Un conjunto de funciones dentro de la entidad de gestión de movilidad de los elementos de la red, conocido como MIHF. El MIHF es la principal entidad de la arquitectura y controla todo el tráfico de información del protocolo.

- Comunicación entre entidades MIHF: distintas entidades MIHF pueden comunicarse entre sí. Por ejemplo, para intercambiar información sobre el estado actual de la red, para ayudar en el proceso de elección de la mejor red para hacer la transición, etc. El estándar IEEE 802.21 especifica interfaces de comunicación entre los usuarios móviles y los puntos de conexión de la red así como entre los elementos internos de la misma. La información se intercambia entre las capas inferiores y las capas superiores, teniendo como punto de referencia el MIHF. De esta forma, puede haber comunicación local (utilizando la misma pila de protocolos) o comunicación remota (entre diferentes entidades MIHF).

- El MIHF ofrece 3 diferentes tipos de servicios, que son necesarios para la comunicación entre las capas inferiores y las capas superiores de la arquitectura general del MIH. La explicación detallada del funcionamiento de estos servicios se recoge en la sección 3.3.

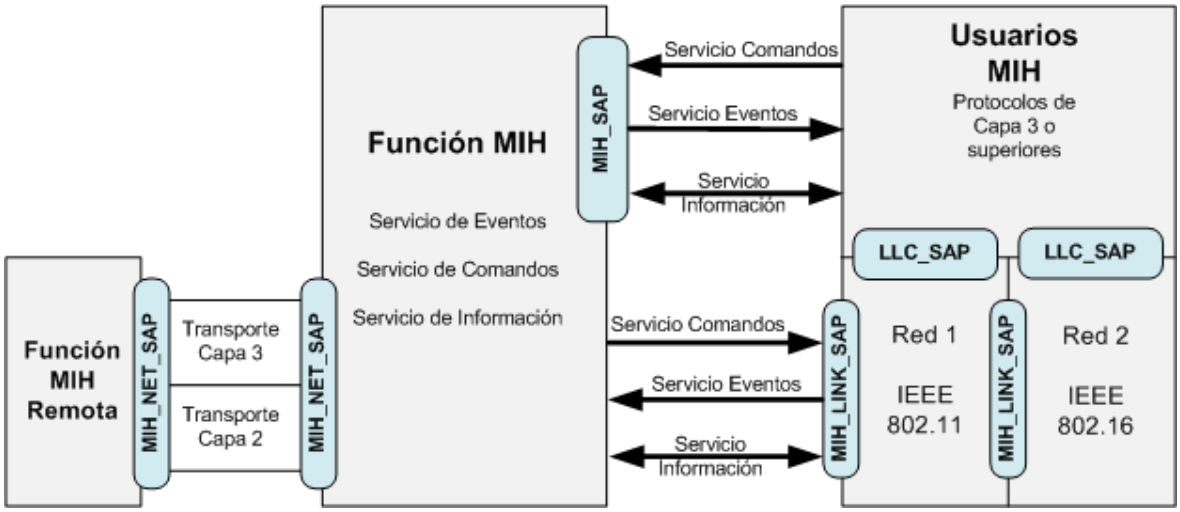

Figura 2.2: Entidades del estándar IEEE 802.21.

2.2. Características

El MIHF, que es la principal entidad de la arquitectura 802.21, ayuda en la toma de decisiones de transición entre redes. Las capas superiores toman decisiones de transiciones y de selecciones de enlaces en base a entradas y al contexto del MIHF. Identificar la necesidad de realizar una transición y determinar la información para que ésta sea eficiente son componentes clave del estándar IEEE 802.21.

Los servicios ofrecidos por el MIHF no dependen de la tecnología de las redes de acceso. La función MIH se comunica con las capas inferiores de la pila del protocolo de gestión de movilidad a través de interfaces de tecnología específica. Estas interfaces se especifican dentro de los estándares correspondientes a las tecnologías de acceso incluyendo IEEE 802.3, IEEE 802.11, IEEE 802.16, 3GPP y 3GPP2.

Según el estándar, distintos factores del usuario o de la red pueden influir en el proceso de transición entre redes. A continuación se muestra un listado de los principales factores a tener en cuenta al iniciar un proceso de transición entre

redes:

- Continuidad del servicio: se define como la no interrupción del servicio durante y después de la transición entre redes con objeto de que la pérdida de datos sea mínima. Todo este proceso debe hacerse sin intervención manual del usuario. Asimismo, el usuario puede ser notificado de que la conexión ha cambiado, pero en ningún momento debe intervenir en el restablecimiento del servicio.

- Tipo de la aplicación: las aplicaciones se comportan de diferente manera ante la pérdida de datos y retrasos en la transmisión. Las aplicaciones que hacen uso de la transmisión de paquetes de datos tienen menos restricciones que las aplicaciones de transmisión de voz y/o vídeo donde se puede notar claramente el retraso o la pérdida de información. Debido a esto tanto el protocolo MIH como la aplicación que se está ejecutando deben ser inteligentes para que el usuario sufra pocas pérdidas de datos y ninguna interrupción de transmisión. Por ejemplo, el retraso en una transmisión de datos utilizando el protocolo FTP apenas se nota, mientras que en una conversación puede que sea necesaria la retransmisión de información.

- Calidad de servicio (QoS): la calidad de servicio utilizada por una aplicación depende de la velocidad, confiabilidad y disponibilidad de la red. La QoS es importante para decidir hacer o no la transición. Por ejemplo, si una aplicación disfruta de una buena QoS en una red y se cambia a una que la tenga peor, la aplicación sufrirá pérdidas de paquetes, retrasos en la transmisión, caída del servicio, etc.

- Descubrimiento de redes: el descubrimiento de redes forma parte de la segunda etapa en el proceso de transición entre redes, que es la etapa de descubrimiento de información, servicios y características de las redes,

independientemente de su tecnología. El tipo de red, identificación de la misma, disponibilidad, calidad, configuración IP, seguridad, etc., son ejemplos de información recibidas por el usuario al hacer un escaneo de redes en su vecindad.

- Selección de la red: el proceso por el cual un nodo elige una red (posiblemente entre varias) para conectarse a nivel de red. Esta selección puede basarse en varios factores: calidad del servicio requerido, preferencias del usuario, coste, políticas de los proveedores de la red, etc.

- Política de transición: el estándar IEEE 802.21 no especifica ningún algoritmo para la selección de la red ya que la selección de la misma es un proceso totalmente dinámico y depende de información real de las redes disponibles. Calidad de servicio, seguridad, retraso, pérdida de paquetes, nivel de sensibilidad de recepción de la señal, velocidad de transmisión, coste, tipo de red, etc., son variables que pueden formar parte de una política de transición. En este trabajo no se hará ninguna especificación del algoritmo de selección de red. Conviene recordar que el objetivo de este trabajo es descubrir redes e información y especificar un sistema de información de movilidad que mejore la transición del usuario móvil en entornos heterogéneos. El algoritmo de selección de red utilizará este servidor de información para tomar la decisión de cambiar entre distintas redes.

Otra característica importante se refiere a la implementación del estándar. Desde 2009, año en el que se estandarizó el protocolo 802.21, varios fabricantes (Intel, Nokia Siemens, NEC, Alcatel-Lucent, etc.) han empezado a implementarlo con el ánimo de verificar y perfeccionar su funcionamiento en entornos reales. Para un correcto funcionamiento del protocolo el IEEE exige lo siguiente:

- El usuario móvil debe ser capaz de soportar múltiples interfaces de red, que pueden ser radios inalámbricos o interfaces de red cableada, o ambas.

- El MIHF es una entidad lógica que puede implementarse tanto en terminales móviles como en elementos fijos de la red (como estaciones base o puntos de acceso). Además, debería funcionar con los equipos ya existentes en el mercado.

- El MIHF de cualquier entidad fija de la red o del terminal móvil debe transmitir y recibir información sobre las condiciones y configuración de las redes que están en su alrededor. Esta información puede originarse en distintas capas de la pila de protocolos dentro del terminal móvil o en uno de los elementos remotos de la red.

2.3. Servicios MIH

El estándar IEEE 802.21 define tres principales servicios que ayudan a mejorar la transición entre distintas tecnologías de redes. Definidos como **Servicio de Eventos** (MIES), **Servicio de Comandos** (MICS) y **Servicio de Información** (MIIS), estos servicios son interfaces de comunicación entre las capas inferiores y superiores de la pila de protocolos del modelo de comunicación. Información detallada de las características del estándar IEEE 802.21 se encuentra en [802.21] y en [Oliva2008]. La Figura 2.3 ilustra el modelo de referencia de comunicación entre las capas del protocolo utilizando los servicios especificados por el estándar.

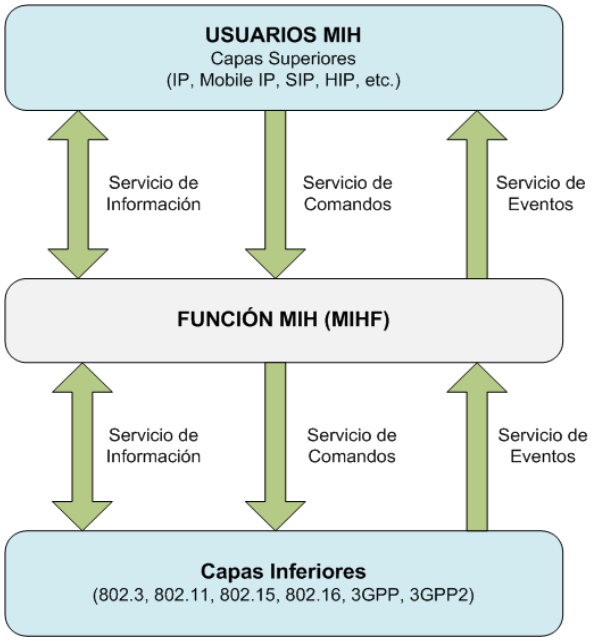

Figura 2.3: Servicios MIH.

Estos servicios, que son ofrecidos por la entidad MIHF, ayudan a los usuarios MIH (las capas superiores) en el mantenimiento de la continuidad del servicio, en la adaptación de la calidad de servicio, en la conservación del nivel de batería del terminal móvil y en el descubrimiento y selección de redes. En cada uno de estos servicios, hay una serie de mensajes que están especificados por el estándar IEEE 802.21. Estos servicios son administrados y configurados por primitivas de administración que son necesarios para el establecimiento de comunicación entre dos entidades MIHF.

De este modo, antes de que una entidad MIHF suministre servicios a otra MIHF, las mismas deben configurarse adecuadamente. Para ello, el estándar especifica 3 etapas denominadas funciones de administración de servicios. Estas 3 funciones son:

1. Descubrimiento de servicios MIH

2. Registro MIH

3. Suscripción a eventos MIH

La función "**Descubrimiento de servicios MIH**" es utilizada por un usuario MIH para descubrir los servicios disponibles en entidades MIHFs local o remotamente. En otras palabras, con este mensaje el usuario puede saber qué servicios (eventos, comandos o información) están disponibles en otra entidad MIH.

La segunda función, denominada "**Registro MIH**", ofrece a una entidad MIH un mecanismo de registro e inscripción en otra entidad MIH. Por ejemplo, un usuario móvil puede enviar este mensaje a un punto de acceso para anunciar su presencia en la red. De acuerdo con el estándar esta función es opcional, así que un nodo puede tener acceso a los servicios de otra entidad MIH sin registrarse previamente.

Por último, y no menos importante, existe la función de "**Suscripción a eventos MIH**". Esta función permite a una MIHF suscribirse a eventos generados por otra MIHF. Por ejemplo, un usuario puede suscribirse a los eventos de las capas física y de enlace de un punto de acceso. Así, si hay algún cambio en la información o propiedades del punto de acceso, automáticamente se envía un mensaje al usuario. Con esta información puede decidir si se cambia de red o no.

La Tabla 2.1 muestra cada una de estas funciones de administración de servicios según el estándar. También se puede ver qué funciones se ejecutan local y/o remotamente.

Función	(L)ocal o (R)emota	Descripción
MIH Capability Discovery	L, R	Descubrir la lista de servicios soportados (eventos, comandos e información) de una MIHF, sea ésta local o remota.
MIH Register	R	Registrar a una función MIHF remota.
MIH DeRegister	R	Cancelar el registro a una función MIHF remota.
MIH Event Subscribe	L, R	Suscribir a uno o más eventos de un MIHF local o remoto.
MIH Event Unsubscribe	L, R	Anulación de la suscripción a uno o más eventos de una MIHF local o remoto.

Tabla 2.1: Funciones de administración de servicios.

2.3.1. Servicio de Eventos Independiente del Medio (MIES)

La decisión de hacer la transición entre dos redes puede iniciarse tanto por el usuario móvil como por alguna entidad de la red. En ambos casos la decisión se toma en base a la información de la red. Comúnmente, esta información proviene de los eventos generados por la capa de enlace, por la capa física o por eventos internos de la MIHF del usuario móvil o de la red. Múltiples usuarios o entidades de la red pueden estar interesados en estos eventos que contienen importante información de la red. De esta forma, estos eventos pueden tener múltiples destinos y las entidades que desean recibir esta información pueden registrarse para saber periódicamente las condiciones de la red. En este apartado se especifica el MIES (del inglés Media Independent Event Service) ofrecido por el estándar IEEE 802.21.

Como ejemplo del funcionamiento de los servicios de eventos se puede imaginar un escenario donde varios nodos móviles están interesados en la

información de un punto de acceso. De esta forma, cuando hay algún cambio en la capa física o en la capa de enlace del punto de acceso (como degradación de la señal), automáticamente se dispara un evento y la información se envía a todos los nodos que se hayan suscrito a este evento.

Cabe mencionar que al recibir un evento, un usuario móvil no está obligado a realizar acción alguna. Es decir, al recibir un evento el usuario puede continuar conectado o decidir cambiarse de red. No está obligado a trasladarse entre redes. El servicio de eventos es meramente informativo y ayuda el usuario a tener información más precisa de las redes.

Los eventos se clasifican como locales o remotos. Un evento local es aquel en el que la información se propaga entre distintas capas dentro de la misma entidad mientras un evento remoto es aquel en el que la información se propaga entre funciones MIHF que están en distintas entidades de la red. La Figura 2.4 ilustra cómo se originan y envían los eventos local y remotamente.

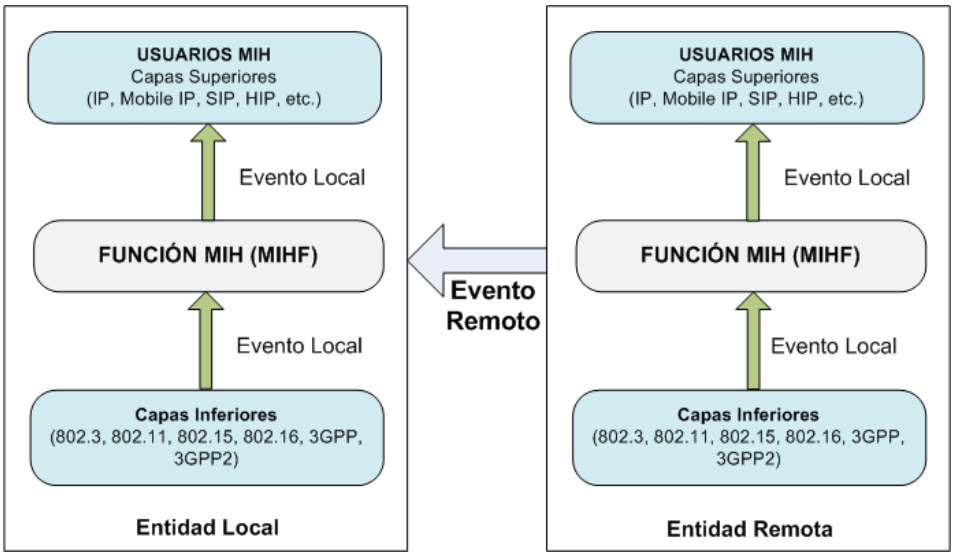

Figura 2.4: Eventos MIH.

Con el ánimo de clarificar el funcionamiento de los eventos en la arquitectura propuesta por el estándar IEEE 802.21 se presenta el siguiente ejemplo.

Supóngase un escenario real en el que un usuario móvil tiene dos interfaces de red activas (una interfaz Wi-Fi y una interfaz Wi-Max) y está conectado a un punto de acceso Wi-Max. Este usuario se suscribe a los servicios generados por las capas inferiores de la entidad local. La interfaz de radio Wi-Fi detecta una nueva red, es decir, recibe una trama beacon (véase la Figura 2.3) con un nuevo identificador de red. Automáticamente se genera un evento local para la función MIHF que retransmite la información al usuario MIH, que puede ser una aplicación VoIP (ej. Skype). En el caso de que la aplicación VoIP desee recibir más información sobre la nueva red se genera un comando para la entidad local solicitando más información.

El estándar soporta una gran cantidad de eventos que se dividen en cinco grandes categorías, que se muestran en la Tabla 2.2.

Tipo de evento	**Descripción**
Cambios en las capas física y/o enlace	Son eventos que corresponden a cambios en las propiedades de las capas física o de enlace. La detección de una nueva red o la caída de un enlace son ejemplos de cambios en las propiedades del nodo. Los mensajes *Link_Up*, *Link_Detected* y *Link_Down* están especificados para este tipo de evento.
Cambios en los parámetros del enlace	Estos eventos se generan cuando ocurre algún cambio en los parámetros de configuración de la capa de enlace. Por ejemplo, uno de los parámetros de configuración puede ser la potencia de recepción de la señal. Un dispositivo recibe la señal del punto de acceso con un valor de -70dB y, en el caso de que este valor llegue a -80dB, se generará un evento y el dispositivo automáticamente lo recibirá.
Predictivo	Son eventos que anuncian la probabilidad de cambios en el enlace en un futuro próximo. Estos eventos se basan en las características anteriores de la red. Por ejemplo, la disminución de la potencia de la señal indica la pérdida de conectividad en un futuro próximo. El mensaje *Link_Going_Down* es un ejemplo de este tipo de evento.

Transición	Estos eventos informan a las capas superiores sobre la ocurrencia de transiciones entre diferentes capas de enlace. Como ejemplo de este tipo de evento están especificados los mensajes *Link_Handover_Imminent* y *Link_Handover_Complete*.
Transmisión	Los eventos de transmisión indican el estado (éxito o fallo) de la transmisión. Este tipo de evento se utiliza por las capas superiores para la administración de la caché cuando ocurre la transición entre redes y todavía hay información pendiente de entregar a la aplicación.

Tabla 2.2: Eventos MIH.

2.3.2. Servicios de Comandos Independientes del Medio (MICS)

El servicio de comandos independientes del medio, conocido como MICS (del inglés, Media Independent Command Service), son comandos enviados por las capas superiores, es decir, por los usuarios MIH, hacia las capas inferiores del modelo de referencia de la arquitectura general del estándar IEEE 802.21 ilustrado en la Figura 2.2. Los usuarios MIH pueden utilizar los comandos para determinar el estado del medio, así como para controlar y configurar el dispositivo móvil con el objeto de tener un óptimo rendimiento. El estado del medio varía de acuerdo con el tiempo y la movilidad del dispositivo. Es por ello que la información del MICS es dinámica y está formada por parámetros de la red como la potencia de la señal y la velocidad de transmisión, entre otros.

La recepción de un comando por parte de una entidad MIH puede generar uno o más eventos. Asimismo, la recepción de un comando anticipa un futuro cambio en las propiedades de alguna interfaz de la entidad receptora, que puede ser un dispositivo móvil o una entidad fija de la red como el punto de acceso o un router. Los usuarios MIH que se hayan suscrito a los eventos de esta entidad recibirán automáticamente un evento de que un cambio inminente

va a ocurrir en alguna interfaz de red. De esta forma, los usuarios MIH pueden prepararse adecuadamente en el caso de que vaya a ocurrir alguna transición.

Como ocurre con los eventos, estos comandos pueden ser locales o remotos. La Figura 2.5 ilustra cómo se originan y envían los comandos local y remotamente.

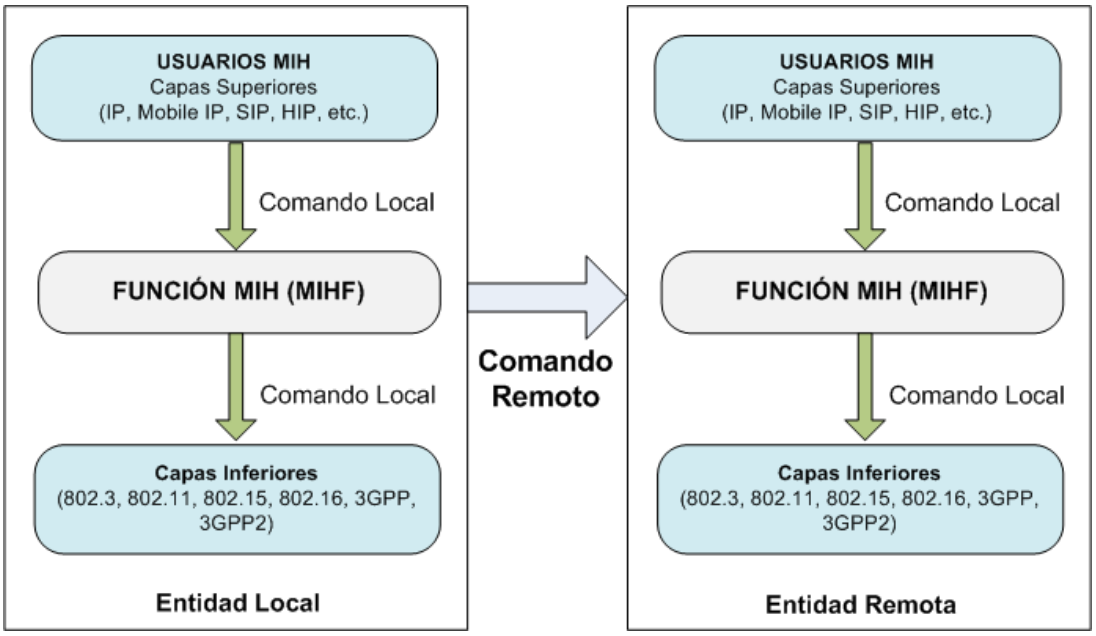

Figura 2.5: Comandos MIH.

En el estándar se definen numerosos comandos. En la Tabla 2.3 se citan los comandos más importantes y que son relevantes para este trabajo.

Comando	Descripción
MIH Link Get Parameters	Obtención de parámetros del medio. Estos parámetros pueden ser la relación señal ruido, el nivel de sensibilidad de recepción de la interfaz, etc.
MIH Link Configure Thresholds	Configuración de umbrales para algunas propiedades o parámetros del enlace.
MIH MN Handover Candidate_Query	Este comando lo utiliza un usuario móvil para averiguar y obtener información de las redes candidatas para una

	futura transición.
MIH MN Handover Commit	Cuando el nodo ya tiene claro cuál será la red elegida para la transición, envía este comando para notificar al servidor MIH la decisión.
MIH N2N *Handover Commit*	Este comando tiene como origen la red del nodo móvil y como destino la red elegida por el nodo. Sirve para informar a la red de destino de que el nodo ha decidido hacer la transición. Con esta información la red de destino puede iniciar la preparación de la transición. Reserva de recursos de calidad de servicio (QoS), autenticación del nodo, verificación del perfil, etc., son algunas de las tareas que la red puede hacer antes de que el nodo inicie la transición.
MIH MN *Handover Complete*	Comando para indicar la finalización de la transición.

Tabla 2.3: Comandos MIH.

2.3.3. Servicio de Información Independiente del Medio (MIIS)

El servicio de información independientes del medio, conocido como MIIS (del inglés Media Independent Information Service), ofrece una arquitectura, donde la función MIHF residiendo en un usuario móvil o en la red puede descubrir y obtener información de todas las redes dentro de una determinada zona geográfica. El objetivo es adquirir una visión global de todas las redes heterogéneas de interés para el usuario móvil en la zona con el fin de facilitar la selección y la transición entre distintas redes. Información como tipo de la red, seguridad, coste de conexión, nombre del operador, localización geográfica del punto de acceso, etc., son algunos de los ejemplos de información que el usuario móvil puede obtener utilizando el servicio MIIS.

Además, el MIIS ofrece una estructura de información y comunicación que permite la transmisión de esta información a través de mecanismos como pregunta/respuesta y suscripción/notificación. El modelo de comunicación del

MIIS contrasta con el modelo de comunicación del MIES y MICS que funcionan de forma asíncrona, es decir, de forma unilateral.

De acuerdo con el estándar, la información de todas las redes (información de movilidad) se almacena en una entidad de red conocida como servidor de información o **servidor MIIS**. Basándose en la información contenida en el servidor MIIS, el usuario móvil puede moverse y hacer transiciones entre distintas redes de forma transparente, conectándose siempre a la mejor red de acuerdo con sus preferencias.

Usualmente, para obtener la información del servidor MIIS el usuario envía un mensaje "*MIH Get Information Request*" y el servidor MIIS responde con un mensaje "*MIH Get Information Response*" con la información solicitada, siendo un mecanismo de pregunta/respuesta. Ambos mensajes están definidos en el estándar IEEE 802.21. Sin embargo, el usuario móvil tiene otras dos alternativas para obtener la información del servidor MIIS. El primer método consiste en obtener la información utilizando el método de suscripción/notificación, donde el usuario hace una suscripción a cualquier cambio en la información almacenada en el servidor. De esta forma, si ocurre un cambio en las prestaciones o características de alguno de los puntos de acceso del operador, todos los usuarios móviles que se haya suscrito al servidor MIIS, automáticamente recibirán un mensaje con información actualizada. Como última alternativa el servidor MIIS puede enviar periódicamente un mensaje en *broadcast* a todos los usuarios conteniendo información de las redes. Cada uno de los métodos anteriormente citados tiene sus ventajas e inconvenientes, lo que depende de las políticas del operador así como de su arquitectura de comunicación de datos y la cantidad de información almacenada por el servidor. En este trabajo se utilizará el mecanismo de pregunta/respuesta, es decir, se hace uso de los dos mensajes especificados por el estándar IEEE 802.21.

El servidor MIIS puede estar en la red local del usuario móvil, en la red

vecina o en una red a varios saltos de distancia. La especificación de este servidor, su funcionamiento, su estructura de almacenamiento, su forma de catalogar la información y los modos de acceso al servidor no se especifican en el estándar IEEE 802.21

Normalmente, la información ofrecida por el MIIS es estática. Parámetros como información del canal, tipo de red, dirección MAC, identificador del operador e información de seguridad del punto de conexión son algunos ejemplos de información. Para que esta información sea accesible a varios usuarios, utilizando diferentes tecnologías, el estándar especifica una estructura común de representación de la información utilizando patrones como el formato XML o codificación binaria.

Para aclarar el funcionamiento del servicio de información imaginemos el siguiente escenario. El MIIS permite que la información sea accesible a cualquier usuario independientemente de la tecnología que esté utilizando. De esta forma, si tenemos un usuario móvil comunicándose a través de la interfaz de red Wi-Fi, el MIIS permite a este usuario conocer información no sólo de las redes Wi-Fi sino también de otras redes como Wi-Max y 3G. De la misma manera, un usuario móvil con una interfaz 3G puede adquirir información de redes Wi-Fi, Wi-Max y 3G. El hecho de conocer información de otras redes permite a un usuario utilizar su interfaz de red activa para descubrir información de otras tecnologías. La gran ventaja es evitar que el usuario tenga que activar una interfaz de red para descubrir servicios y redes en la vecindad, con el consiguiente ahorro de energía y procesamiento.

El MIIS soporta una gran variedad de elementos de información (IE, del inglés Information Elements) que ayudan al usuario móvil a elegir la mejor red. Los IE se dividen en tres grandes grupos. A continuación se muestra las principales características de cada grupo:

- **Información general e información específica de cada red de acceso**: este grupo contiene información general de las diferentes redes que estén en el rango de cobertura. Por ejemplo, una lista de las redes disponibles y sus correspondientes operadores, acuerdos de *roaming* entre operadores, el coste de la conexión a la red, la seguridad y la calidad del servicio son algunos ejemplos de información que se almacena en este grupo.

- **Información específica del punto de conexión**: este grupo proporciona información sobre los diferentes puntos de conexión (PoA, del inglés Point of Attachment) de cada una de las redes de acceso disponibles, incluyendo información como las configuraciones de red de un PoA, su ubicación geográfica, velocidades de transmisión soportadas, el tipo de capas física y de enlace y parámetros de los canales. En este grupo también están incluidos los servicios de capa superior y capacidades individuales de cada PoA.

- **Otra información**: este grupo contiene información específica de las redes de acceso, sus servicios específicos e información propietaria de los fabricantes.

La Tabla 2.4 ilustra estos grupos y su contenido. Un MIIS no necesariamente debe tener toda esta información almacenada pues los IE son opcionales.

Elemento de Información	Descripción
Información General	
IE_Network_Type	Tipo de las redes de acceso que están disponibles en una zona geográfica determinada.
IE_Operator_Type	Identificador del operador de la red de acceso.
IE_Service_Provider_ID	Identificador del proveedor de servicios.
IE_Country_Code	Identificador del país.
Información Específica de cada red de acceso	
IE_Network_ID	Identificador de la red de acceso.
IE_Roaming_Partners	Operadores de red con los que la red actual tiene acuerdos de *roaming* directo.
IE_Cost	Indicación de coste de servicio o el uso de la red.
IE_Network_QoS	Características de calidad del servicio de la red.
IE_Network_Data_Rate	El valor máximo de la velocidad de transmisión de datos soportado por la capa de enlace de la red de acceso.
IE_Net_Frequency_Bands	Las bandas de frecuencias soportadas por la red.
IE_Net_IP_CFG_Methods	Métodos de configuración de direcciones IP soportados por la red de acceso.
IE_Net_Mob_Mgmt_Prot	Tipo de protocolo de administración de movilidad soportado.
Información Específica del punto de conexión	
IE_PoA_Link_Addr	Dirección de la capa de enlace del PoA
IE_PoA_Location	Localización geográfica del PoA.
IE_PoA_Channel_Range	Rango de frecuencias soportados por el PoA.
IE_PoA_IP_Addr	Dirección IP del PoA.
Otra información	
Vendor Specific IEs	Información propietaria de los fabricantes.

Tabla 2.4: Elementos de Información (IE).

La Figura 2.6 muestra los diferentes IE y un mapa global de las diferentes redes en una zona geográfica.

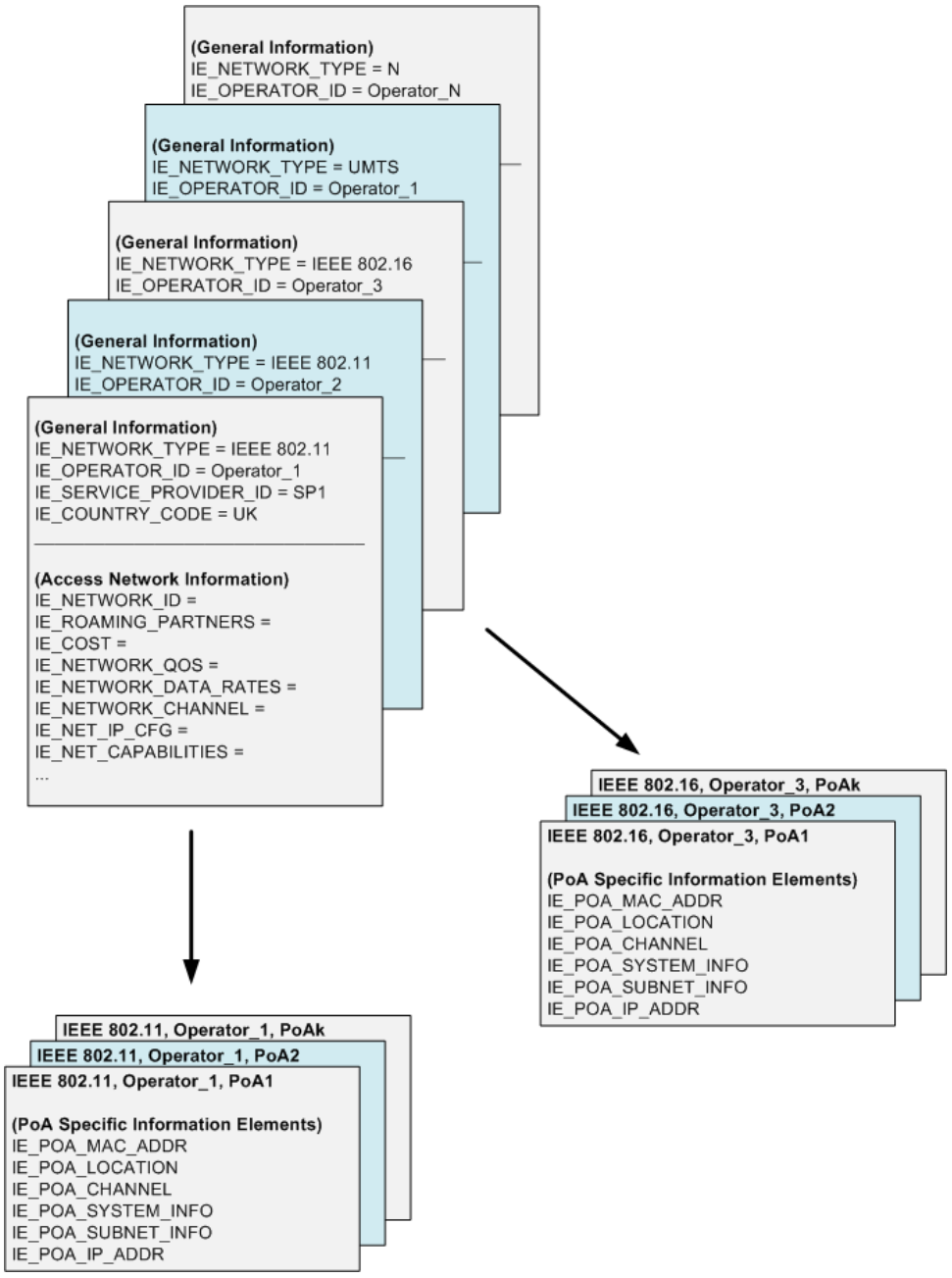

Figura 2.6: Mapa Global del Servicio de Información.

En la Figura 2.6 se puede ver que distintos operadores soportan una determinada tecnología de red. De este modo el soporte a la red IEEE 802.11 lo proporciona el Operator_1 y el Operator_2. Un único operador también soporta

múltiples tecnologías de red. Así el Operator_1 soporta redes IEEE 802.11 y UMTS mientras que el Operator_3 soporta las redes IEEE 802.16 y UMTS. Los elementos de información general se especifican para cada red soportada por un operador. Así, en el caso del Operator_1 la información general de la red se especifica para las redes IEEE 802.11 y redes UMTS, mientras que en el caso del Operator_2 se especifica solamente para la red IEEE 802.11.

2.4. Escenario Común de Movilidad

La Figura 2.7 muestra una transición entre una red Wi-Fi y una red Wi-Max. Se asume que el usuario móvil posee dos interfaces de red donde ambas pueden transmitir y recibir información simultáneamente. El ejemplo se divide en tres fases que son (iniciación, preparación y ejecución), para facilitar la comprensión. El escenario tiene los siguientes elementos: un dispositivo móvil con dos interfaces de red (Wi-Fi y Wi-Max), un punto de acceso Wi-Fi, un punto de acceso Wi-Max y un servidor MIIS que contiene información de las dos redes.

Actualmente, el usuario está conectado a la red Wi-Fi y hace una transición a la red Wi-Max sin pérdida de conectividad, es decir, todas las aplicaciones que estén siendo ejecutadas en la red Wi-Fi pasarán a la red Wi-Max sin que el usuario apenas note el cambio. Seguidamente se describen cada una de las tres etapas, ilustrando los mensajes intercambiados entre las entidades de la red.

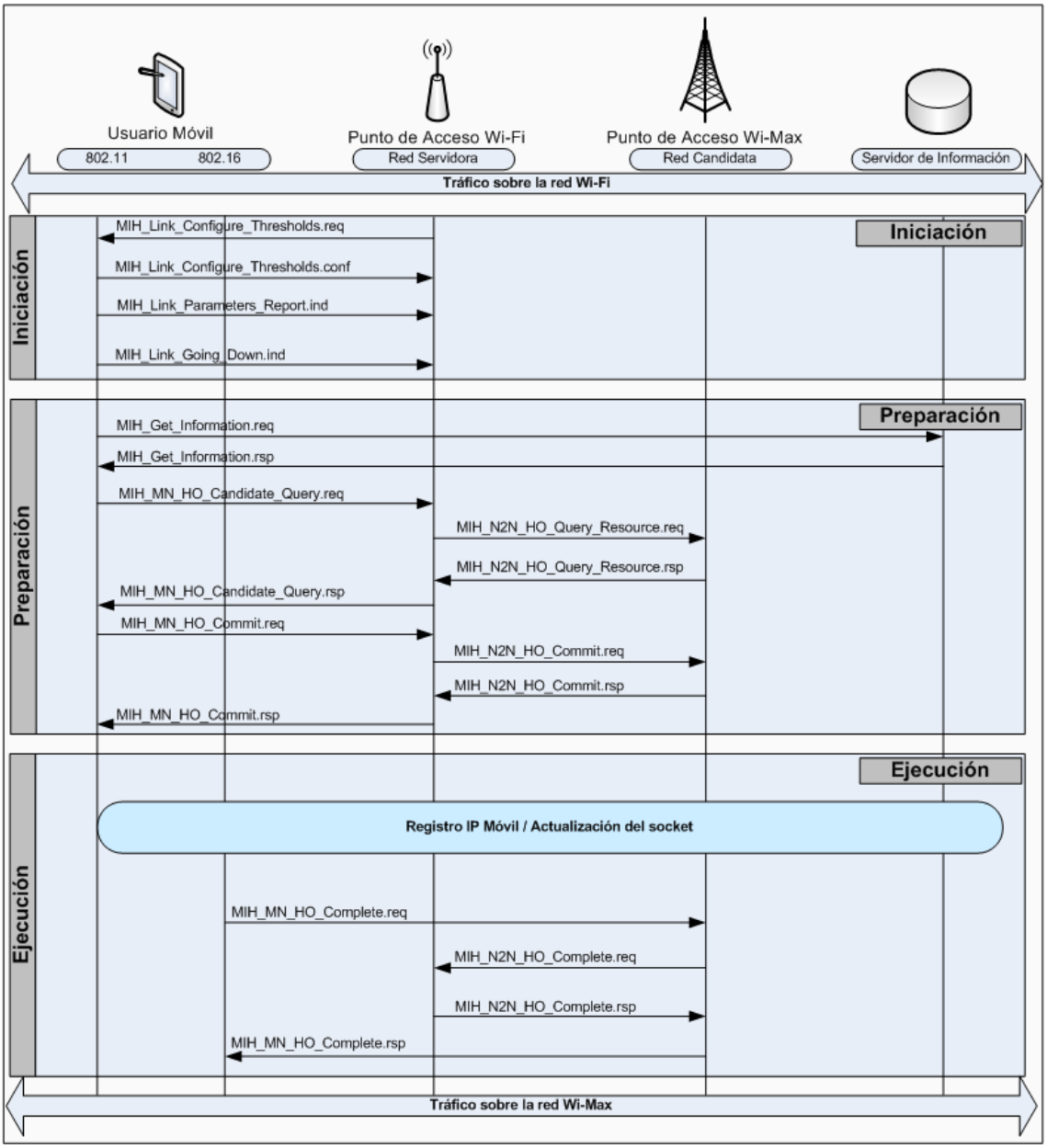

Figura 2.7: Ejemplo de una transición entre una red Wi-Fi y una red Wi-Max.

1. Iniciación de la transición: en esta primera fase el usuario móvil está conectado a la red Wi-Fi, teniendo lugar toda la comunicación a través del punto de acceso. La principal función de la fase de iniciación es identificar la necesidad de hacer una transición. Para ello, el usuario MIH (MIHU) del punto de acceso configura la interfaz Wi-Fi del usuario con algunos umbrales referentes a la calidad de servicio del enlace a través del envío del mensaje *MIH_Link_Configure_Thresholds.req*. En un momento dado el

usuario móvil envía un mensaje *MIH_Link_Parameters_Report.ind* con información del estado del enlace inalámbrico a todos los MIHU registrados (uno en este caso). Este mensaje se genera cuando algún parámetro de configuración sobrepasa el umbral configurado para la interfaz. Estos valores pueden ser la potencia de la señal, la velocidad de transmisión de datos, el retardo de la red, etc. Este tipo de evento indica que el usuario puede perder conectividad con el punto de acceso a corto plazo. Así que cuando la señal se degrada de forma considerable y el punto de acceso ya no puede garantizar las necesidades de calidad de servicio al usuario, el usuario envía el mensaje *MIH_Link_Going_Down.ind* al MIHU del punto de acceso. Esta notificación, indica que probablemente se perderá la conectividad a nivel de capa de enlace en un determinado intervalo de tiempo. Este mensaje contiene dos campos importantes: (1) intervalo de tiempo (en milisegundos) que especifica el tiempo en el cual la interfaz perderá conectividad y (2) la causa por la que se perderá la conectividad. Normalmente es una indicación al usuario móvil de que una transición va a ocurrir próximamente. Después de recibir el mensaje, el punto de acceso Wi-Fi está habilitado para iniciar una transición antes de que el usuario pierda la conexión. En resumen, en esta primera fase se realiza la configuración de umbrales de calidad de servicio y la medición del estado del enlace del usuario móvil.

2. Preparación de la transición: una vez detectada la necesidad real de realizar la transición, se inicia la segunda etapa que es la de preparación. El objetivo de esta fase es buscar las redes disponibles, verificar las características y condiciones del enlace y ejecutar un algoritmo de decisión para elegir alguna de las candidatas. En primer lugar, el usuario móvil envía un mensaje *MIH_Get_Information_req* al servidor MIIS solicitando información de las redes vecinas. El servidor MIIS responde enviando un mensaje *MIH_Get_Information_rsp* indicando al usuario que hay redes

disponibles. Una vez que el usuario recibe la respuesta del servidor MIIS, pasa a tener una visión general de las redes vecinas y sus principales características como tipo de tecnología, nombre del proveedor de servicios de telecomunicaciones, coste, QoS, canales de transmisión, etc. Posteriormente, el usuario realiza un escaneo de las redes para certificar de que éstas están disponibles para conexión. Tras realizar el escaneo, averigua los recursos de las redes disponibles, enviando el mensaje *MIH_MN_HO_Candidate_Query.req* al punto de acceso Wi-Fi que encamina el mensaje al punto de acceso Wi-Max. En la Figura 2.7 sólo hay un punto de acceso candidato, que es el punto de acceso Wi-Max. Sin embargo, el mensaje se envía a todos los puntos de acceso de las redes candidatas que haya en la vecindad. La finalidad es identificar la disponibilidad de recursos en las redes candidatas como QoS, coste, ancho de banda y configuraciones de red. Además, utilizando este mensaje, el usuario puede descubrir la dirección IP del punto de acceso, antes de hacer la transición entre las dos redes. El punto de acceso Wi-Max contesta la solicitud del usuario a través del mensaje *MIH_N2N_HO_Query_Resource.*rsp. Es importante recordar que la verificación de disponibilidad de recursos se puede hacer con varias redes y varios puntos de acceso. Al final de esta fase el usuario tiene suficiente información de las redes candidatas y ya puede tomar la decisión correcta del punto de acceso candidato a elegir. Al tener la información de los recursos disponibles en cada red y en cada punto de acceso y el resultado del escaneo, el punto de acceso Wi-Max es seleccionado como la red de destino. En el caso de que los recursos no estén disponibles en la red de destino, el usuario puede sufrir algún retardo o corte en la comunicación. La última etapa de la fase de preparación es la reserva de recursos de la red a la que va a conectarse. Para la reserva de recursos el usuario envía el mensaje *MIH_MN_HO_Commit.req* al punto de acceso Wi-Fi, que contacta directamente con el punto de acceso Wi-Max. Éste contesta con el mensaje

MIH_MN_HO_Commit.rsp y finaliza la etapa de preparación de la transición.

3. Ejecución de la transición: durante esta fase, se realiza la transición entre las redes Wi-Fi y Wi-Max. El protocolo de movilidad (Mobile IPv4, Mobile IPv6, etc.) se encarga de gestionar toda la comunicación de una tecnología a otra, es decir, las sesiones activas que existan en la interfaz de red Wi-Fi se transfieren a la interfaz de red Wi-Max. Esto significa que, en este momento, las dos interfaces (Wi-Fi y Wi-Max) están activas, lo que minimiza el tiempo de transición entre las redes. Una vez que la comunicación haya sido transferida a la nueva red y los recursos de la interfaz antigua hayan sido liberados, se deshabilita la interfaz Wi-Fi del usuario móvil. Al transferir toda la comunicación de la interfaz Wi-Fi a la interfaz Wi-Max, el usuario confirma la transición enviando el mensaje *MIH_MN_HO_Complete.req* al punto de acceso Wi-Max. El punto de acceso Wi-Max envía un mensaje de confirmación *MIH_N2N_HO_Complete.req* al punto de acceso Wi-Fi comunicándole la nueva conexión a nivel de red del usuario móvil. Éste responde enviando el mensaje *MIH_N2N_HO_Complete.rsp* de vuelta al punto de acceso Wi-Max que lo reenvía finalmente al usuario móvil a través del mensaje *MIH_MN_HO_Complete.rsp*. A partir del envío de estos cuatro mensajes de esta fase, el intercambio de información se realiza a través de la red Wi-Max.

2.5. Trabajos Relacionados

Durante los últimos años el estándar IEEE 802.21 ha aglutinado a un gran número de investigadores. Los esfuerzos se han centrado principalmente en dos temáticas:

- Utilizar el estándar para optimizar las transiciones entre redes heterogéneas.

- Analizar la funcionalidad del servicio MIIS.

Esta última temática puede dividirse, a su vez, en dos: por un lado, la formulación de propuestas que utilizan la información proporcionada por el servicio MIIS, y por otro, aquellas otras que versan sobre el concepto, funcionamiento y arquitectura del servicio MIIS. Seguidamente se analiza la literatura más relevante en cada una de las temáticas consideradas.

Respecto a utilizar el estándar para optimizar las transiciones entre redes heterogéneas cabe destacar los siguientes trabajos:

[Cacace2006] especifica una entidad centralizada denominada "Gestor de Movilidad" que se comunica con las capas inferiores del estándar IEEE 802.21 y que es responsable de ocultar la heterogeneidad de las redes al usuario final. A través de una experimentación real los autores demuestran que utilizando el estándar y el gestor de movilidad propuesto, el usuario logra mejores transiciones y obtiene mayor rendimiento en una comunicación utilizando el protocolo VoIP (del inglés *Voice over IP*).

[Lampropoulos2008] propone el uso del estándar IEEE 802.21 para atender las necesidades de calidad del servicio ó QoS (del inglés *Quality of Service*) del usuario móvil de forma que apenas se note una mínima interrupción en las transiciones. Asimismo, se especifican los mensajes que se intercambian las entidades cuando un usuario realiza una transición entre dos puntos de acceso. Por último, se menciona que algunos aspectos no son cubiertos por el estándar como, por ejemplo, el mecanismo de seguridad, el algoritmo de decisión de transición y la ejecución de la transición a nivel de capa de red.

[Pontes2008] utiliza los servicios del estándar IEEE 802.21 para abordar la integración de las redes Wi-Fi y Wi-Max, centrándose en el intercambio de mensajes entre el usuario y las entidades de red. También se describen arquitecturas y futuros escenarios para redes móviles y para redes inalámbricas heterogéneas con múltiples saltos.

[Taniuchi2009] describe los servicios del estándar IEEE 802.21 contemplando algunos escenarios de movilidad en entornos heterogéneos. Asimismo, aborda cuestiones de implementación en Java y Linux, lo que facilita la interoperabilidad. Por último, expone los principales desafíos que surgen a la hora de implementar el estándar comentando cómo lograr la aceptación y el despliegue del nuevo estándar.

Finalmente, [Lampropoulos2010] propone la integración de las redes Wi-Fi y Wi-Max analizando la petición y reserva de recursos a nivel de capa de enlace y la gestión de energía del terminal móvil. Para ello plantea un cambio en el estándar IEEE 802.21 haciendo énfasis en la asignación de primitivas entre el estándar IEEE 802.21 y las diferentes capas de interconexión con otras tecnologías de red y en las mejoras de los estándares relacionados.

Respecto a la información proporcionada por el servicio MIIS merecen mención especial los siguientes trabajos:

[Wu2006] presenta un algoritmo de decisión de transición basado en el perfil de usuario. Este algoritmo utiliza el servidor MIIS para obtener información de red como dirección de enlace e información del estado del enlace para una óptima selección de la red destino. Los resultados de la simulación, que describe un caso de uso utilizando prioritariamente redes Wi-Fi, demuestran que el usuario realiza mejores transiciones y sufre menos pérdida de paquetes utilizando el algoritmo propuesto.

[Seol2007] propone una interesante solución para transiciones verticales entre redes Wi-Max y 3GPP gracias a un novedoso mecanismo de gestión de movilidad, en el que el usuario móvil puede hacer transiciones aunque no tenga el protocolo IP Móvil instalado. Sin embargo, requiere importantes cambios relativos a la estructura de la red y a las entidades participantes en el proceso de transición.

[Mussabir2007] diseña un mecanismo que optimiza el protocolo de movilidad IPv6 Móvil Rápido [FastMIP] en redes VANET (del inglés *Vehicular Ad Hoc Networks*) gracias a los servicios MIH. Para ello define un servidor MIIS que almacena tanto información estática (coste, tipo de red, identificador del operador, etc.) como dinámica (ancho de banda, calidad de servicio, usuarios conectados, tasa de errores del enlace, etc.) de las redes vecinas. El trabajo permite concluir que la utilización del protocolo IPv6 Móvil Rápido conjuntamente con los servicios que ofrece el estándar IEEE 802.21 mejora notablemente el tiempo de transición.

[Floroiu2007] contempla la integración de los servicios MIH en un Subsistema Multimedia IP (IMS) con el fin de optimizar la calidad de servicio extremo a extremo. Su arquitectura transversal considera el intercambio de información entre servidores MIIS relativa a la calidad y al coste del servicio, especificándose dos tipos de servidores MIIS: uno en el operador al que está conectado el usuario y otro perteneciente al otro operador. Se asume que los servidores MIIS tienen un acuerdo de nivel de servicio y que intercambian información relevante. Sin embargo, no se proporciona especificación alguna de la infraestructura de servidores MIIS, detalles de su funcionamiento, tipo de información almacenada y protocolo de comunicación entre servidores.

[Yoo2008] muestra un esquema que utiliza el retardo medio de comunicación entre puntos de acceso vecinos como parámetro de decisión a la hora de hacer una transición. Con esta información almacenada en un servidor MIIS central el

usuario puede estimar el tiempo de entrega de la información requerida y decidir el mejor momento para cambiar de red. El trabajo hace un análisis detallado del coste de obtener esta información de un servidor MIIS, teniendo en cuenta factores como el número de saltos entre el usuario y el servidor, el retardo del enlace en cada una de las tecnologías utilizadas, el tiempo de procesamiento del servidor MIIS para la entrega de la información y el tiempo que el usuario necesita para hacer un barrido en diferentes tecnologías.

[Baek2008] especifica un mecanismo de handover entre redes UMTS y Wi-Max utilizando el servidor MIIS con información relevante de las redes vecinas como es la calidad de servicio de las mismas. Para facilitar la continuidad del servicio cuando el usuario se desplaza entre redes se recurre a un nuevo mecanismo que consta de tres pasos: medición de la calidad de servicio, reserva pasiva de los recursos y activación de la reserva. La simulación realizada en NS-2 permiten concluir que el mecanismo propuesto mejora la transición del usuario y garantiza la calidad de servicio requerida por el mismo.

[Liu2009] introduce un nuevo algoritmo de decisión de transición basada en una función del coste de conexión de la red (información ésta proporcionada por el servidor MIIS) bastante flexible que permite balancear diferentes factores en la toma de decisión y mejorar la eficiencia energética de las transiciones.

[Christakos2009] explora el servicio MIIS permitiendo que un usuario se autentique con la red de destino mientras está conectado a su red actual, disminuyendo así el tiempo de transición. Esto es posible puesto que los *routers* de la red se registran en el servidor MIIS utilizando un nuevo mensaje denominado MIH Set *Information Request* que contiene información como la localización geográfica del router, su dirección IP, información de la capa de enlace, distancia a los *routers* vecinos, etc. Una vez que el servidor MIIS tiene almacenada la información de los *routers* de la red, el usuario puede utilizarla y realizar una autenticación previa, mejorando así el rendimiento en las

transiciones.

[Lim2009] descubre los puntos de acceso Wi-Fi haciendo uso del servidor MIIS, lo que posibilita que el usuario pueda obtener información de las diversas redes Wi-Fi a través de un interfaz común, independientemente del tipo de red a la que esté conectado actualmente. Este nuevo esquema de descubrimiento, que no requiere ninguna modificación de los protocolos existentes, se basa en que el servidor MIIS proporciona al usuario una lista de canales utilizados por los puntos de acceso vecinos. Al recibir el mensaje de respuesta del servidor el usuario lleva a cabo un procedimiento de barrido selectivo en vez de realizar un barrido completo, reduciendo así el tiempo de detección de redes.

[Liu2009_2] utiliza una función de coste para realizar una selección óptima de la red destino con la información proporcionada por el servidor MIIS. Esta propuesta, muy similar a la presentada anteriormente ([Liu2009]), consigue una mejora significativa en el consumo de energía a la hora de moverse entre redes vecinas mediante la utilización del servidor MIIS, ya que el usuario realiza un barrido selectivo en vez de un barrido total de los canales de las redes. Un aspecto a tener en cuenta es la utilización del acelerómetro del dispositivo móvil como punto de inicio para la realización del barrido. En otras palabras, si el acelerómetro se activa, significa que el usuario ha empezado a moverse y que debe realizar un barrido para detectar redes vecinas. Por el contrario, si el acelerómetro no se activa, el usuario no está realizando movimiento alguno, no buscando nuevas redes con el consiguiente ahorro de energía.

Finalmente, [Khan2011] plantea el uso del servicio MIIS para que el usuario adquiera la información del canal de configuración y luego la utilice para analizar un conjunto limitado de canales utilizados por los puntos de acceso vecinos en lugar de hacer un barrido de todos los canales posibles, lo que retrasaría la transición. Como el punto de acceso y el usuario móvil deben ser equipos que posean características de localización geográfica, su alcance es

bastante limitado, no siendo válida esta solución en escenarios genéricos con servidores MIIS, ya que actualmente no todos los equipos inalámbricos gozan de esta funcionalidad.

Respectos a trabajos relativos al concepto, especificación y arquitectura del servicio MIIS cabe reseñar los siguientes:

[Kutscher2006] y [Kutscher2006a] introducen los denominados "mapas de servicios", que permiten a un usuario móvil obtener una visión detallada de las redes disponibles y de los servicios que ofrecen en función del contexto del usuario (posición geográfica, rutas de movilidad, etc.) y de los requisitos de las aplicaciones. No utilizan necesariamente el servidor MIIS del estándar, proponiendo una arquitectura general de servidores de información de movilidad con sus elementos de información. La experimentación realizada utilizando datos reales de puntos de acceso de una determinada zona de la ciudad de Berlín demuestra que el usuario hace mejores transiciones utilizando los mapas de servicio.

[Giaffreda2007] y [Pentikousis2007] mejoran la gestión de la movilidad gracias a las denominadas "Redes de Ambiente" (del inglés, *Ambient Networks*), una infraestructura que tiene el objetivo de recolectar y almacenar información de las redes vecinas a través de diferentes dominios. Ambos contemplan la creación de una entidad denominada DNISI (del inglés *Dynamic Networks Information Service Infrastructure*), que tiene por objeto recopilar y correlacionar la información de diversas capas de la pila de protocolos y a través de diferentes dominios. Asimismo, demuestran, mediante diversos experimentos, que el concepto de *Ambient Networks* puede tener cabida perfectamente en las redes de nueva generación.

[Ying2008] especifica un mecanismo de gestión de movilidad que utiliza el servidor MIIS para recopilar información de las capas de enlace y de aplicación

de las redes vecinas ofreciendo así información relevante al usuario. La solución propuesta soporta transiciones dentro del mismo operador así como entre diferentes operadores. La principal aportación de este trabajo es que el usuario y el punto de acceso colaboran para que el servidor MIIS tenga información dinámica de las redes (información del enlace, características de calidad de servicio, historial del usuario y condiciones de la red).

[Kim2010] presenta un mecanismo donde los usuarios envían periódicamente información dinámica de los enlaces al servidor de información MIIS. Por tanto, siempre que los usuarios se mueven envían al servidor información detallada del estado del enlace de cada uno de los puntos de acceso. Almacenando la calidad de la señal en diferentes puntos se puede calcular de manera estadística la calidad en otro punto. Los usuarios utilizan esta información para tomar la mejor decisión a la hora de hacer una transición.

[Vogueler2011] propone una arquitectura distribuida de servidores MIIS donde los usuarios móviles administran la información almacenada en el servidor MIIS. La arquitectura responde a una estructura jerárquica de tablas DHT (del inglés *Distributed Hash Table*) con múltiples niveles o capas donde cada usuario mantiene su propio servidor MIIS y todos los nodos están interconectados. La estructura DHT permite reducir la latencia de señalización en el descubrimiento de redes vecinas. Como DHT es completamente distribuido, la estructura jerárquica introduce escalabilidad y tolerancia a fallos, siendo una interesante alternativa para una implementación de un servidor MIIS centrada en el usuario.

[Neves2011] considera un servidor de información que contempla el almacenamiento de información dinámica (recursos disponibles en tiempo real) de las redes de acceso. La principal aportación de este trabajo es que los puntos de acceso envían la información dinámica de forma periódica. Así, cuando el usuario obtiene información del servidor MIIS, ésta está actualizada no siendo

necesario realizar una comprobación de recursos en todas las redes, ahorrando tiempo y energía en las transiciones en escenarios heterogéneos.

Finalmente, [Buiati2010] [Buiati2011] [Buiati_FGCN2011] especifica un sistema de información de movilidad que reduce el tiempo de descubrimiento de redes vecinas y mejora la calidad de los *handovers* entre redes de distintas tecnologías y con diferentes operadores. El sistema propuesto considera la división de las redes de acceso en zonas geográficas de movilidad, clasificadas de forma jerárquica y administradas por distintos tipos de servidores MIIS: MIIS Zonal, MIIS Local y MIIS Global.

2.6. Síntesis del Capítulo

El principal objetivo de este capítulo ha sido revisar los conceptos y características del proceso de transición en redes heterogéneas. Además, se ha hecho una detallada descripción del estándar IEEE 802.21 que contempla una arquitectura inteligente que permite la transición entre redes heterogéneas.

Se ha visto que el estándar define tres tipos básicos de servicios (eventos, comandos e información) que proporcionan inteligencia en capa de enlace y otra información de red relativa a las capas superiores para optimizar la transición entre redes heterogéneas. Estas redes pueden ser 3GPP, 3GPP2 y las redes pertenecientes a la familia IEEE 802: 802.3 (Ethernet), 802.11 (Wi-Fi) y 802.16 (Wi-Max).

Asimismo, se ha visto un ejemplo de una transición entre una red Wi-Fi y una red Wi-Max haciendo énfasis en el intercambio de mensajes entre el usuario móvil y los puntos de acceso de ambas redes. Conviene tener presente que la principal aportación de este trabajo es la especificación del servidor de información dando características como su ubicación, su funcionamiento, su

estructura de almacenamiento, su comunicación con otros servidores, su forma de catalogar la información y los modos de acceso al servidor por el usuario final. Toda esta información se trata en detalles en el siguiente capítulo.

3. SISTEMA JERÁRQUICO DE INFORMACIÓN DE MOVILIDAD

Este capítulo describe la especificación de un sistema de información de movilidad. En primer lugar, se define el modelo conceptual del sistema, donde se expone un modelo genérico de movilidad. Luego, se especifican tres tipos de servidores de información, un MIIS Zonal que atiende a los usuarios de una determinada zona geográfica, un MIIS Local que controla varias zonas de movilidad de un operador y un MIIS Global que permite la comunicación entre diferentes operadores.

El sistema jerárquico de información de movilidad contempla la movilidad de los usuarios por distintas redes y múltiples operadores. Así, en el MIIS Global se especifica un modelo de acuerdo de nivel de servicio que permite que dos o más operadores intercambien información de movilidad.

También, se hace una comparativa entre las principales características de cada servidor MIIS respecto a la arquitectura, despliegue, escalabilidad, tiempo de respuesta al usuario móvil y sus posibles ubicaciones físicas dentro de un ambiente con múltiples redes de acceso y operadores. Asimismo, se especifican algunos escenarios para validar la propuesta. El capítulo finaliza con una breve síntesis de lo expuesto en el mismo.

3.1. Introducción

Como se ha comentado en el capítulo anterior, la idea de dividir las redes de acceso en zonas de movilidad y que éstas sean administradas por diferentes servidores MIIS, permite que el usuario obtenga información de movilidad y haga mejores transiciones tanto en lo que se refiere a la calidad como al retraso

total de los mismos. Un punto importante en la gestión de información entre diferentes entidades en un ambiente de redes es el deseo de compartir la información por parte de las mismas. Si las entidades no cooperan entre sí de alguna forma, en ningún momento el usuario podrá tener una visión general de la información. Por ello, en este capítulo además de especificar tres tipos de servidores MIIS, también se especifica un modelo de acuerdo de nivel de servicio donde los distintos tipos de servidores MIIS en los diferentes niveles de la jerarquía pueden compartir información de movilidad.

3.2. Modelo Conceptual

En este apartado, se define el modelo conceptual del sistema de información de movilidad. Se pretender dar una definición del modelo que sea lo más genérico posible para que el sistema pueda ser utilizado en diferentes escenarios de movilidad.

Como se puede ver en la Figura 3.1, el sistema de información de movilidad está dividido en tres niveles. En primer lugar se definen m zonas de movilidad *i* *(i = 1, 2, …, m)*, siendo i el identificador de una zona de movilidad en una determinada área geográfica. En este primer nivel se establecen *m* servidores $\boldsymbol{MIISZonal_i}$ *(i = 1, 2, …, m)*, siendo i el identificador del servidor MIIS Zonal en una determinada zona geográfica. En el segundo nivel se especifican *m* servidores $\boldsymbol{MIISLocal_i}$ donde *(i = 1, 2, …, m)*, siendo *i* el identificador del servidor MIIS Local. Por último, en el tercer nivel se especifican *m* servidores $\boldsymbol{MIISGlobal_i}$ donde *(i = 1, 2, …, m)*, siendo *i* el identificador del servidor MIIS Global.

Una pregunta habitual cuando se habla de una estructura jerárquica de información, es la relativa a la cantidad de servidores que debe tener la jerarquía y qué información debe estar presente en los diferentes niveles de la

estructura. Respecto al número de puntos de acceso, zonas de movilidad y servidores MIIS **por operador**, el $MIISZonal_i$ *(i = 1, 2, …, m)*, puede controlar y almacenar información de m PoA_j *(j = 1,2,…, m)*, siendo j el identificador del punto de acceso. El $MIISLocal_i$ *(i = 1,2,…, m)* puede gestionar m *MIISZonalj* donde *(j = 1,2,…, m)*, siendo j el identificador del servidor MIIS Zonal. El $MIISGlobal_i$ *(i = 1)* puede gestionar m $MIISLocal_j$ donde *(j = 1,2,…, m)*, siendo j el identificador del servidor MIIS Local. Conviene reseñar que se ha especificado un servidor MIIS Global por operador y no m servidores como en los niveles inferiores. Este servidor tiene el rol de representar al operador en la comunicación con los servidores MIIS Global de los otros operadores. Por tanto, toda la parte de inteligencia y acuerdos de servicios que deben existir entre dos o más operadores se hace únicamente en el servidor MIIS Global, no sobrecargando los servidores MIIS de los niveles inferiores cuando dos operadores no tienen ningún tipo de acuerdo de servicio.

Los usuarios están conectados a los puntos de acceso, y, éstos, a su vez, están conectados a los servidores MIIS Zonal. Los servidores MIIS Zonal están conectados y se comunican con los servidores MIIS Local, que a su vez, están conectados con el servidor MIIS Global. Por último, el servidor MIIS Global del operador se comunica con otros servidores MIIS Global a través de un *backbone* común o a través de Internet.

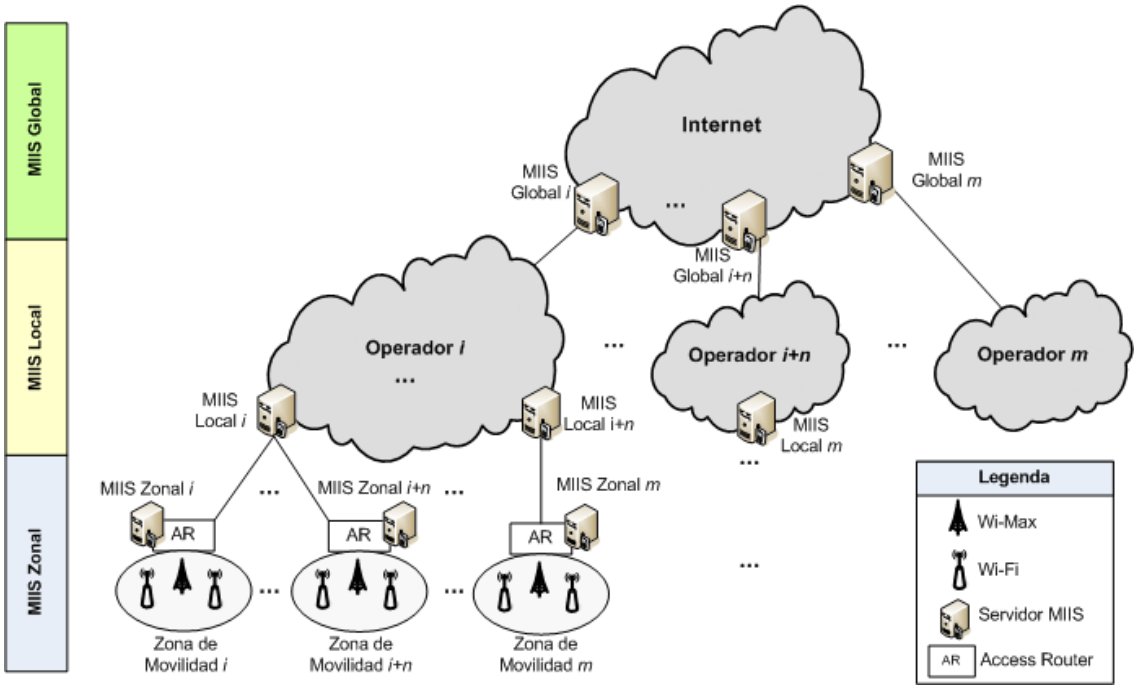

Figura 3.1: Modelo conceptual del sistema de movilidad.

3.3. Servidor MIIS Zonal (MIIS Zonal)

Un servidor MIIS Zonal es un servidor MIIS que tiene almacenado toda la información de movilidad de las redes y de los puntos de acceso de una determinada zona o región de un operador. La división de las redes de acceso en zonas o regiones se debe al hecho de que un operador normalmente tiene cobertura en toda una ciudad o mismo en todo un país, siendo demasiada información para ser administrada por un único servidor MIIS. De esta forma, un servidor MIIS Zonal puede administrar varias redes de acceso de diferentes tecnologías y un operador puede tener varios servidores MIIS Zonal donde los usuarios móviles pueden acceder a la información. El algoritmo de funcionamiento de cómo el usuario obtiene la información del servidor MIIS Zonal se ilustra en la Figura 3.2.

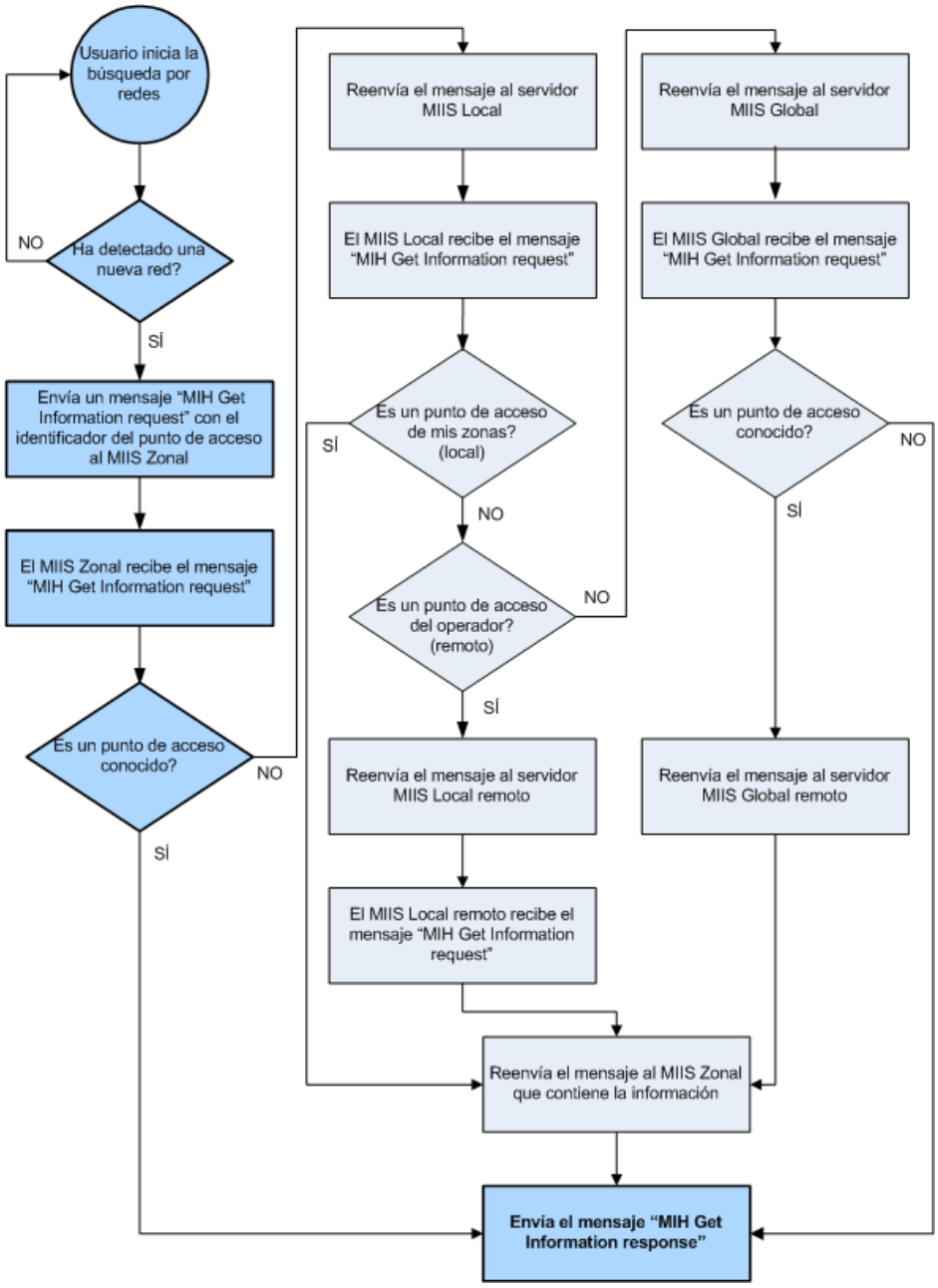

Figura 3.2: Algoritmo de funcionamiento del servidor MIIS Zonal.

Utilizando el servidor MIIS Zonal, el usuario puede llevar a cabo una transición entre dos redes perteneciendo ambas al mismo operador y siendo administradas por un servidor MIIS Zonal común.

En primer lugar, el usuario inicia la búsqueda de nuevas redes a través del método de escaneo o barrido. Si hay alguna red en la vecindad, el usuario

recibe un mensaje (un evento *MIH Link Detected*) de la capa inferior del protocolo, lo que significa que se ha detectado una nueva red. Tras recibir este mensaje, el usuario envía un mensaje *MIH Get Information request* (conteniendo el identificador del punto de acceso detectado) (PoA_ID, del inglés *Point of Attachment Identification*) al servidor MIIS Zonal con el objetivo de obtener más información del mismo, ya que la detección de una red sea por escaneo activo o pasivo no ofrece mucha información al usuario. Al recibir la solicitud, el servidor MIIS Zonal comprueba si el punto de acceso detectado está registrado en su base de datos, y si es el caso, envía un mensaje *MIH Get Information response* con información detallada del punto de acceso al usuario. Si el punto de acceso no está registrado o pertenece a otra zona, el servidor MIIS Zonal reenvía la solicitud al servidor MIIS inmediatamente superior en la jerarquía.

Conviene señalar que, por un lado, la gran mayoría de los puntos de acceso Wi-Fi no son administrados por los operadores habituales, no están registrados en ningún servidor MIIS y son administrados por pequeños locales comerciales (por ejemplo restaurantes, cafeterías, etc.) y por empresas (por ejemplo Starbucks, McDonald's, EMT Madrid, etc.). Así, si se detecta uno de estos puntos de acceso y se envía la petición de información al servidor MIIS Zonal, el usuario no recibe información adicional del mismo por no estar registrado en el servidor MIIS. Por otro lado, en los últimos años varios operadores de telecomunicaciones detectaron un gran incremento en el uso de la tecnología 3G, que tiene limitadas prestaciones (velocidad de conexión, ancho de banda y cobertura). Para reducir la sobrecarga de estas redes y ofrecer más calidad de servicio al usuario, los operadores están trabajando con comunidades de redes Wi-Fi, donde el usuario puede hacer el handover entre las dos tecnologías de forma automática. Un ejemplo de este tipo de cooperación son las redes [BT-FON] (British Telecom y Fon España). En un acuerdo entre estas dos compañías, la operadora BT ofrece a sus clientes más de 2 millones de puntos de acceso FON Wi-Fi en todo el Reino Unido. Por lo tanto, el usuario puede

desplazarse de la red 3G hacia la red Wi-Fi de forma automática y transparente. La tendencia actual es que el número de puntos de acceso Wi-Fi gestionados por operadores siga aumentando de forma importante en los próximos años. Así, cada vez habrá más puntos de accesos Wi-Fi registrados en algún servidor MIIS, lo que beneficiará la experiencia móvil del usuario.

En la Figura 3.3 se puede ver un escenario con varios servidores de información MIIS Zonal que gestionan diferentes zonas de movilidad en un entorno con múltiples operadores. En su desplazamiento el usuario utiliza el servidor MIIS Zonal en la tarea de descubrimiento de las redes vecinas y hace una transición intra-zonal, es decir, se mueve a la cobertura de un punto de acceso perteneciente a la misma zona de movilidad.

En este escenario tenemos dos operadores. Cada operador tiene un servidor MIIS Global, dos servidores MIIS Local y tres servidores MIIS Zonal. Describiendo los elementos de la Figura en orden ascendente, los puntos de acceso están divididos en seis zonas de movilidad. Cada una de ellas es administrada por un MIIS Zonal diferente. En el operador 1 el servidor MIIS Local 1 controla el servidor MIIS Zonal 1 y el servidor MIIS Zonal 2, y el servidor MIIS Local 2 controla el servidor MIIS Zonal 3. En el operador 2 el servidor MIIS Local 3 controla los servidores MIIS Zonal 4 y MIIS Zonal 5, y el servidor MIIS Local 4 controla el servidor MIIS Zonal 6. En el nivel superior de la jerarquía está el servidor MIIS Global 1 que se comunica con el MIIS Global 2 y permite que el usuario haga una transición entre el Operador 1 y el Operador 2 y viceversa.

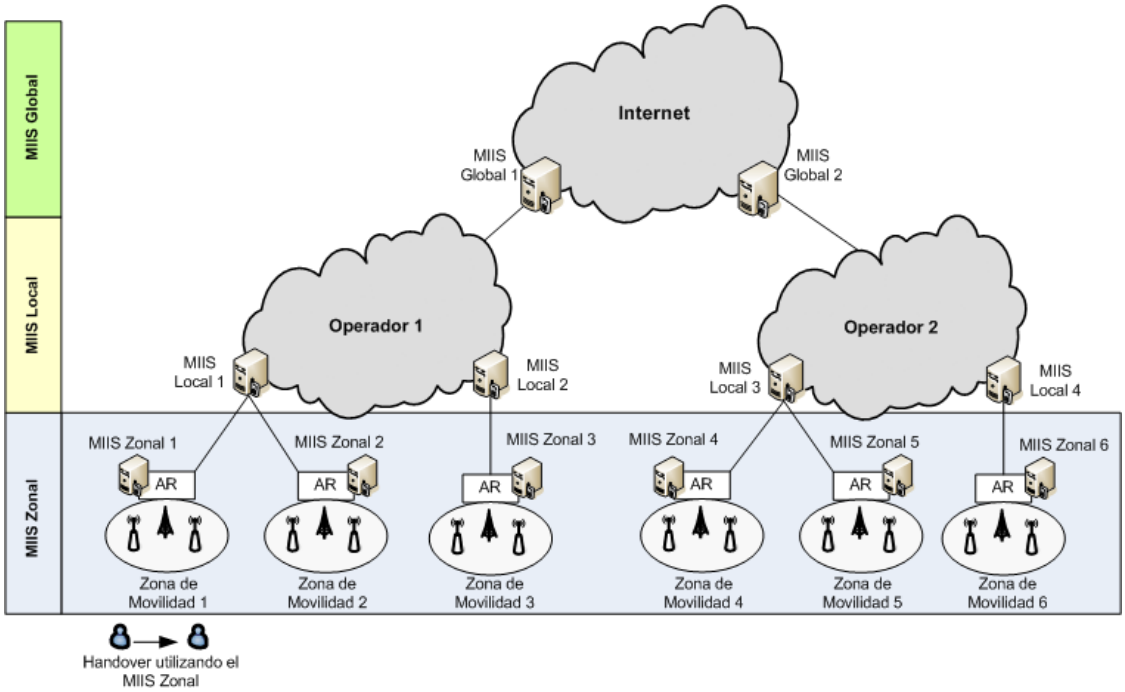

Figura 3.3: Ubicación física del servidor MIIS Zonal.

Tres son los requisitos para el despliegue de un servidor MIIS. Para el servidor MIIS Zonal tenemos las siguientes características:

1. **Ubicación física del servidor MIIS Zonal**: el servidor MIIS Zonal estaría ubicado físicamente en el primer *router* después del punto de acceso al cual el usuario está conectado de forma inalámbrica. Este *router* también se denomina AR (*Access Router*). Comúnmente, el usuario está a dos o tres saltos de distancia del servidor MIIS Zonal, lo que permite al usuario una rápida respuesta a su solicitud de información de movilidad. Por lo tanto, el servidor MIIS Zonal es el servidor más cercano al usuario móvil. Mientras más veces el usuario pueda utilizar este servidor para obtener información, independientemente de su posición geográfica, mucho mejor.

2. **Información almacenada en el servidor MIIS**: dado que un servidor MIIS Zonal tiene un control total sobre la información de las redes y de los puntos de acceso de su zona, en este tipo de servidor los usuarios móviles tienen acceso a toda la información de los puntos de acceso no existiendo

ninguna restricción relativa a la información de las redes del operador. Por lo tanto, el usuario puede saber a través de un mensaje *MIH Get Information request*, información como QoS, coste del servicio, seguridad, velocidad de transmisión, localización geográfica de los PoA, etc. El MIIS Zonal es el único servidor de información que almacena toda la información posible de un punto de acceso.

3. **Periodicidad del envío de la información a los usuarios por parte del servidor MIIS**: la información del servidor MIIS Zonal sólo se envía cuando el usuario envía un mensaje *MIH Get Information request* con un identificador del punto de acceso detectado.

3.3.1. Elementos de Información

El servidor de información MIIS Zonal tiene información detallada de todos los puntos de acceso de una determinada zona. En la Figura 3.4 se indican los elementos de información que puede contener un servidor de información MIIS Zonal.

Figura 3.4: Elementos de Información de un Servidor MIIS Zonal.

En Información General el servidor MIIS Zonal almacena información general del operador como el nombre, el identificador, el código del país, etc. En Información de la Red se almacena la información de las tecnologías de red presentes en el operador así como información del coste de uso, calidad de servicio, acuerdos de roaming, protocolos de movilidad soportados, etc. Por último el grupo Información del Punto de Acceso contiene información relativa a un punto de acceso específico como su dirección IP, canales de transmisión, localización geográfica, etc. En el sistema de información de movilidad propuesto, se ha creado un elemento de información, el IE_Zone_ID relativo a la zona de movilidad del punto de acceso. Todos estos elementos de información se refieren a un operador, a sus redes y a sus puntos de acceso. En el caso de que un operador tenga más de una tecnología de red y más de un punto de acceso, hay varios grupos de información.

Conviene diferenciar el concepto de red con punto de acceso. Varios puntos de acceso pueden constituir una única red. Por ejemplo, un operador o una empresa prestadora de servicios de red implementa una red inalámbrica en un aeropuerto con decenas de puntos de acceso y todos llevan el mismo nombre. Hay, por tanto, una única red y varios puntos de acceso.

3.3.2. Señalización

La Figura 3.5 muestra la señalización que existe entre el usuario móvil y el servidor MIIS Zonal cuando el usuario está haciendo una transición dentro de la misma zona, es decir, entre dos puntos de acceso administrados por el mismo servidor MIIS Zonal.

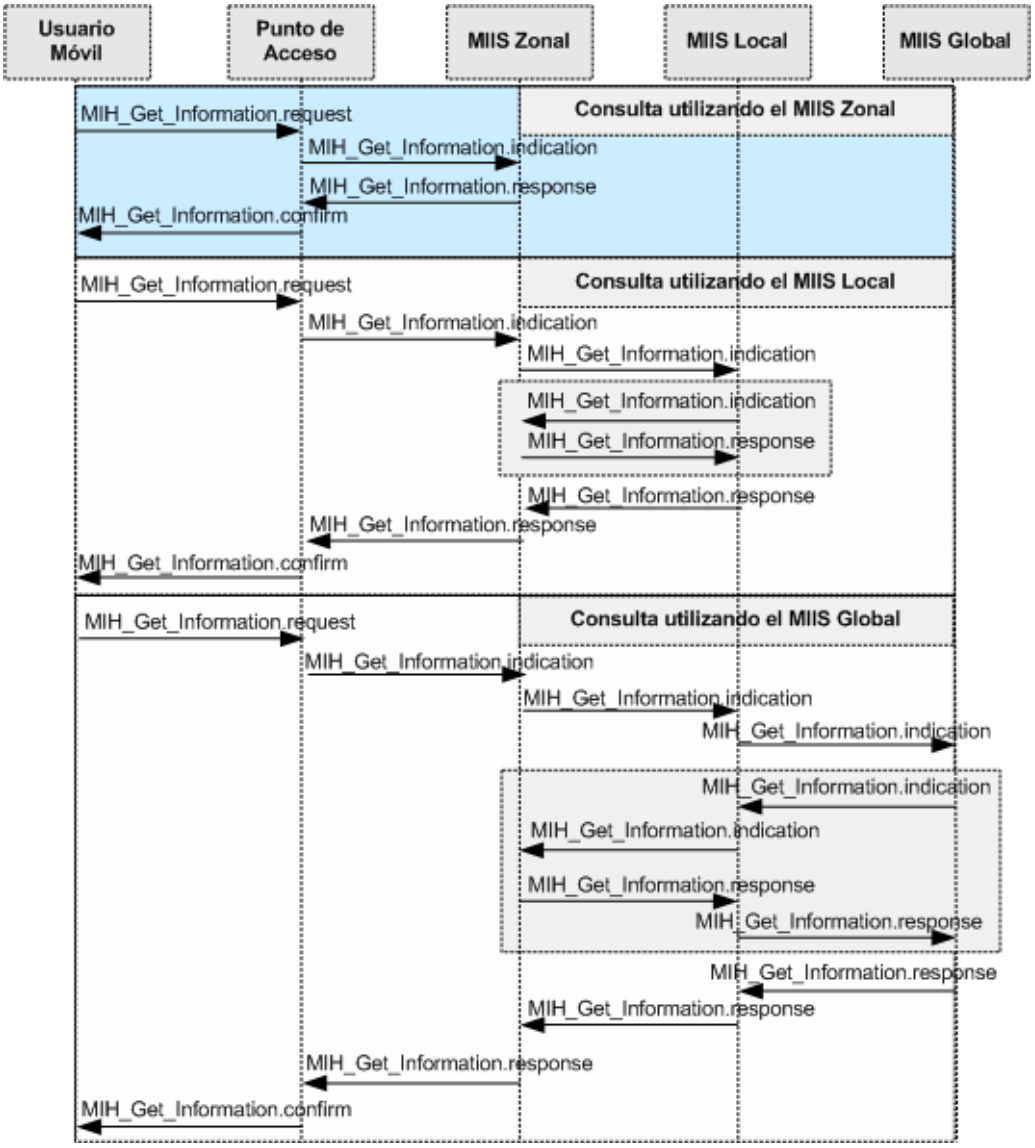

Figura 3.5: Comunicación entre el usuario y el MIIS Zonal.

Como ya se ha comentado, cuando el usuario quiere obtener más información de un determinado punto de acceso, se envía un mensaje *MIH Get Information request* conteniendo el identificador del punto de acceso detectado al MIIS Zonal de su zona. Al recibir la solicitud del usuario, el servidor MIIS Zonal comprueba si el punto de acceso detectado está registrado en su base de datos. Si lo está, envía el mensaje de respuesta *MIH Get Information* response con información detallada del punto de acceso al usuario. Si el punto de acceso detectado pertenece a la misma zona a la que está ubicado el usuario, el servidor MIIS Zonal contestará con información detallada del mismo. Una gran

ventaja que presenta este sistema de información de movilidad frente a propuestas existentes es que además de enviar la respuesta al usuario con información del punto de acceso detectado, el servidor MIIS Zonal también envía la información de todas las redes y puntos de acceso de una determinada zona. Así, el usuario no necesita enviar más solicitudes al servidor MIIS en el caso de que detecte más redes de acceso en la misma zona.

La comunicación entre el usuario y el servidor MIIS Zonal se resume en 4 mensajes. El primer mensaje, el *MIH Get Information request* con el identificador del PoA detectado (POA_ID), se envía cuando el usuario detecta una nueva red. Este mensaje se envía al punto de acceso que está conectado el usuario. El punto de acceso reenvía el mensaje al servidor MIIS Zonal (renombrándolo como *MIH Get Information indication*). El MIIS Zonal recibe el mensaje y responde al punto de acceso a través del mensaje *MIH Get Information response*. Este mensaje se reenvía al usuario final como *MIH Get Information confirm*.

El despliegue de uno o más servidores de información MIIS Zonal presenta importantes ventajas para el usuario. La primera es que el usuario sólo recibe información relativa a su zona de movilidad, disminuyendo el tamaño del mensaje *MIH Get Information response*. Como el mensaje de respuesta contiene información de los puntos de acceso de la zona, el usuario no tiene que enviar nuevamente la solicitud al servidor MIIS cuando se detecta nuevas redes pertenecientes a la misma zona. La otra ventaja es que como el servidor MIIS Zonal está ubicado físicamente dentro del operador, el usuario tiene acceso directo a la información, disminuyendo el retardo en el descubrimiento de redes vecinas y en la obtención de la información de las mismas.

Por último, una característica bastante interesante y útil del servidor MIIS Zonal, es que se puede enviar al usuario la información general de varias redes de una determinada zona cuando éste se conecta por primera vez a la red. Así, teniendo conocimiento de qué redes están disponibles en una zona geográfica,

el usuario puede apagar las interfaces que no se utilizarán, ahorrando energía y optimizando su funcionamiento.

3.4. Servidor MIIS Local

El servidor MIIS Local es un servidor MIIS que puede administrar el intercambio de información entre diversos servidores MIIS Zonal pertenecientes a un mismo operador. El MIIS Local no almacena información detallada de las redes de acceso de un operador, sino que únicamente mantiene un listado de los servidores MIIS Zonal y sabe perfectamente donde están las redes de acceso basándose en los identificadores de las mismas, actuando como *proxy*. De esta forma, un servidor MIIS Local puede gestionar la comunicación entre varios servidores MIIS Zonal donde los usuarios móviles pueden acceder a la información.

Cuando un usuario móvil desea saber más información de un punto de acceso, envía una solicitud directamente a su MIIS Zonal. El MIIS Zonal consulta en su base de datos si el punto de acceso detectado (POA_ID) está registrado. Si la consulta está relacionada con algún punto de acceso que está fuera de su zona, es decir, no lo tiene registrado en la base de datos, el MIIS Zonal reenvía la petición al servidor MIIS que está en el nivel superior de la jerarquía, que es el MIIS Local. Este servidor mantiene un listado de todos los puntos de acceso de la red y sus respectivas zonas de movilidad. Una vez que el MIIS Local recibe la petición del servidor MIIS Zonal, puede realizar tres acciones diferentes:

1. **Responder (localmente)**: el MIIS Local responde localmente cuando el punto de acceso detectado pertenece a una de sus zonas de movilidad.

2. **Encaminar a un MIIS Local (remoto)**: el MIIS Local verifica en su tabla si

el POA_ID pertenece a su operador. Si es el caso, el MIIS Local contacta al MIIS Local remoto que sabe a qué MIIS Zonal encaminar la petición. El MIIS Zonal contesta al usuario con información detallada de la red solicitada.

3. **Encaminar al MIIS Global**: el MIIS Local toma otra acción en el caso de que el POA_ID no pertenezca al mismo operador, encaminando la petición al MIIS Global del operador.

El algoritmo que describe cómo el usuario obtiene la información del servidor MIIS Local se ilustra en la Figura 3.6. Utilizando el servidor MIIS Local, el usuario puede llevar a cabo una transición entre dos redes, perteneciendo ambas al mismo operador y siendo administradas por diferentes servidores MIIS Zonal.

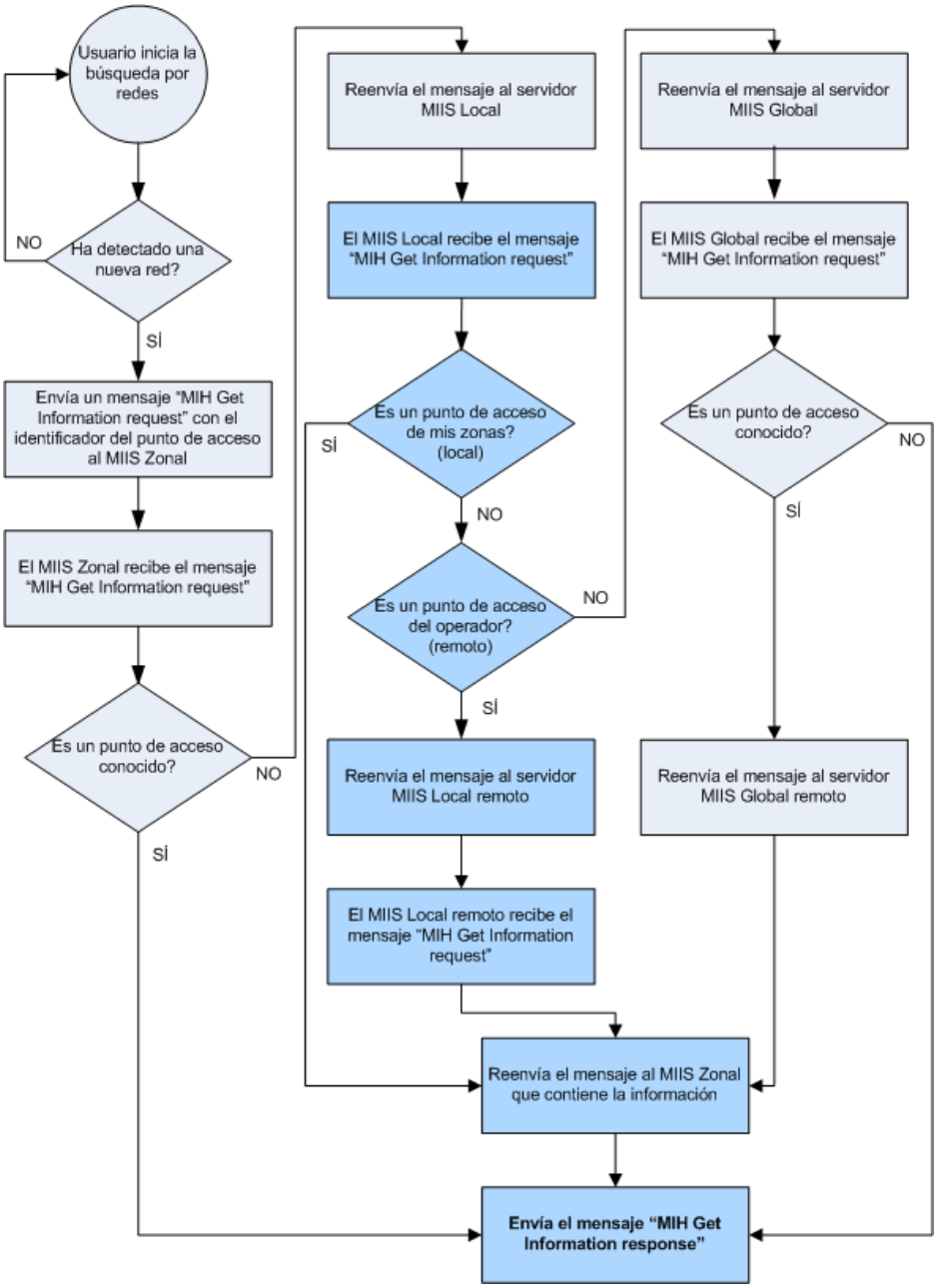

Figura 3.6: Algoritmo de funcionamiento del servidor MIIS Local.

En la Figura 3.7, se muestra un escenario con dos servidores de información MIIS Local que gestionan diferentes zonas de movilidad en un entorno con múltiples operadores. En este escenario el usuario hace dos transiciones utilizando el MIIS Local. En la primera transición, el usuario se desplaza de la Zona 1 a la Zona 2, zonas que son gestionadas por el mismo MIIS Local. De esta forma, el MIIS Local contesta locamente a la petición del usuario. En la segunda

transición, el usuario se desplaza de la Zona 2 a la Zona 3, zonas que son gestionadas por diferentes servidores MIIS Local. En este caso el MIIS Local 1 encamina la petición al MIIS Local 2, siendo una respuesta remota, ya que proviene de otro MIIS Local.

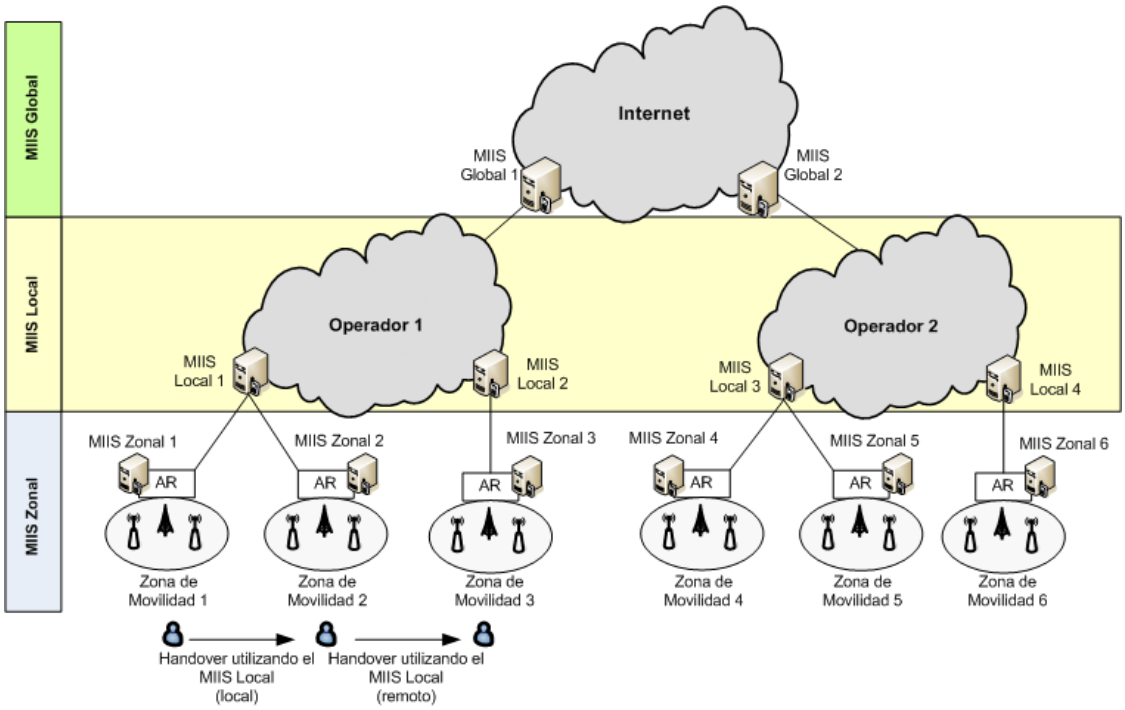

Figura 3.7: Ubicación física del servidor MIIS Local.

La determinación del número ideal de servidores MIIS Local que un operador debe tener depende de una gran cantidad de variables como (número de usuarios en cada zona de movilidad, número de puntos de acceso, extensión geográfica del operador, etc.). Es decir, la especificación de un número dado de servidores MIIS Local depende exclusivamente de la arquitectura de red implementada por el operador. Lo importante aquí es la especificación funcional de los diferentes tipos de servidores MIIS.

Como se ha comentado en la sección 4.2, tres son los requisitos para el despliegue de un servidor de información. Para el servidor MIIS Local tenemos las siguientes características:

1. **Ubicación física del servidor MIIS Local**: el servidor MIIS Local está ubicado físicamente en el núcleo de la red del operador, permitiendo el acceso a la información a usuarios ubicados en las diferentes zonas de movilidad del operador. Comúnmente, el usuario móvil se ubica de entre tres a seis saltos de distancia del servidor MIIS Local.

2. **Información almacenada en el servidor MIIS**: dado que un servidor MIIS Local no almacena información detallada de las redes, en este tipo de servidor se almacena principalmente un listado que contiene el identificador de las redes y a qué zona corresponde cada una de ellas.

3. **Periodicidad del envío de la información a los usuarios por parte del servidor MIIS**: la información almacenada en el servidor MIIS Local sólo se utiliza cuando un usuario móvil quiere obtener más información de un punto de acceso que no está en su zona de movilidad.

3.4.1. Elementos de Información

El servidor de información MIIS Local almacena menos información que el servidor MIIS Zonal al tratarse de un servidor que actúa como proxy. En la Figura 3.8 se indican los elementos de información que puede contener un servidor de información MIIS Local.

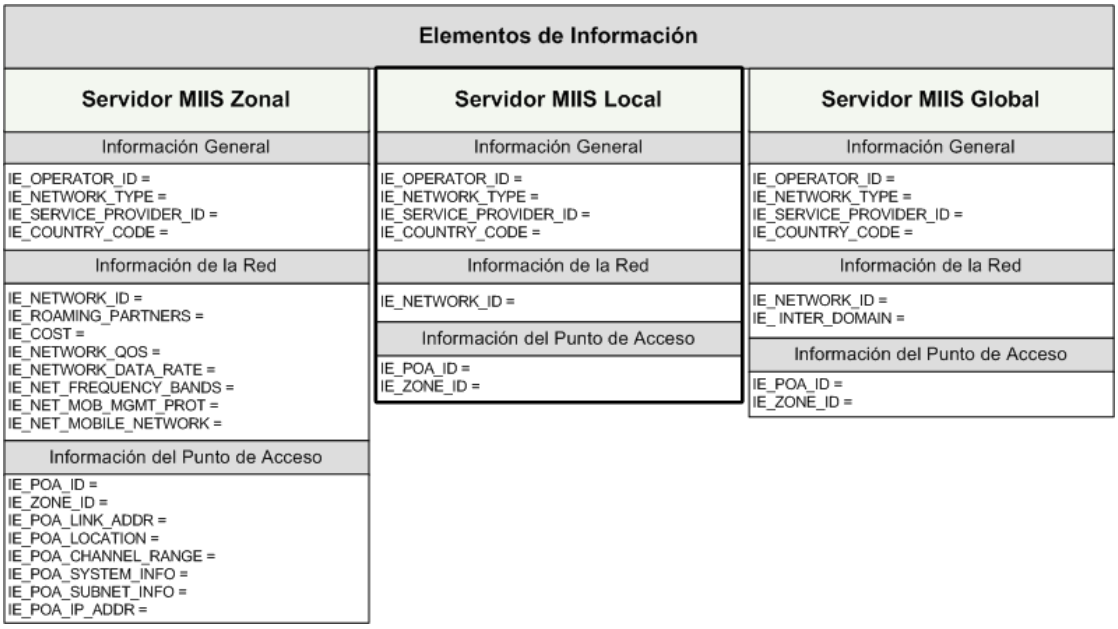

Figura 3.8: Elementos de Información de un servidor MIIS Local.

En Información General el servidor MIIS Local almacena información del operador como su nombre, su identificador, el código del país, etc. En Información de la Red se almacena únicamente el identificador de la red. Por último, el grupo Información del Punto de Acceso contiene el identificador del punto de acceso IE_PoA_ID y el IE_Zone_ID que sirve para que el servidor MIIS Local encamine la consulta de información al MIIS Local remoto apropiado, que se la enviará al servidor MIIS Zonal que contiene información detallada del punto de acceso detectado por el usuario móvil.

3.4.2. Señalización

Solamente hay comunicación entre el usuario y el servidor MIIS Local cuando el usuario detecta un punto de acceso que no pertenece a su zona de movilidad. La Figura 3.9 muestra la comunicación que debe existir entre el usuario móvil y el servidor MIIS Local cuando el usuario está haciendo una transición entre distintas zonas de movilidad, es decir, entre dos puntos de acceso administrados por dos distintos servidores MIIS Zonal, gestionados o no por el mismo servidor MIIS Local.

En la comunicación entre el usuario y el servidor MIIS Local, el primer mensaje, el *MIH Get Information request*, se envía cuando el usuario detecta una nueva red. Este mensaje se envía al punto de acceso al que está conectado el usuario. El punto de acceso reenvía el mensaje al servidor MIIS Zonal (renombrándolo como *MIH Get Information indication*). Por su parte, este último lo reenvía al servidor MIIS Local que sabe a quien corresponde la solicitud; lo reenvía al servidor MIIS Zonal que contiene la información del punto de acceso detectado o al servidor MIIS Local remoto. El MIIS Zonal que almacena la información solicitada por el usuario responde enviando el mensaje *MIH Get Information* response, que hace el camino inverso pasando por el servidor MIIS Local, servidor MIIS Zonal, punto de acceso y llegando al usuario final como *MIH Get Information confirm.*

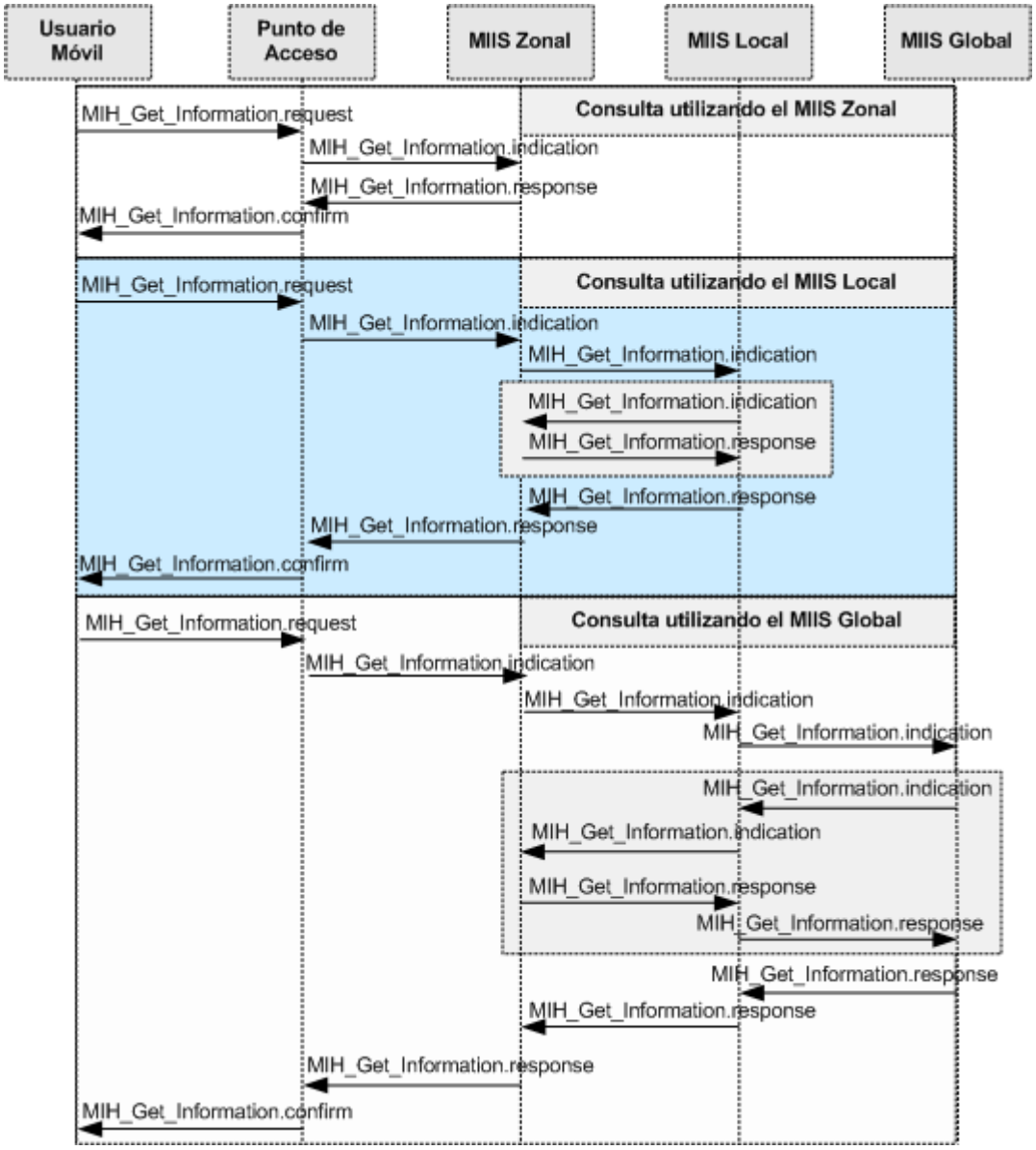

Figura 3.9: Comunicación entre el usuario y el MIIS Local.

La utilización de un MIIS Local presenta en tres grandes ventajas para el usuario (1) ll MIIS Local tiene una visión general de todas las zonas y redes de acceso de un operador, por lo que sabe a dónde reenviar la solicitud de información del usuario (2) Al intercambiar información entre diferentes zonas, el servidor puede ofrecer más posibilidades de handovers al usuario móvil y (3) El MIIS Local está habilitado para utilizar mecanismos de optimización (como caché), lo que reduce el intercambio de mensajes en el backbone del operador.

3.5. Servidor MIIS Global

El último tipo de servidor MIIS se utiliza en ambientes con múltiples operadores. Su principal función es intercambiar información entre diferentes operadores y permitir que el usuario haga transiciones entre dos o más operadores. En este escenario se deben hacer dos consideraciones (1) para que haya intercambio de información entre dos operadores, lo primero que debe hacerse es determinar y especificar qué información puede intercambiarse cada servidor MIIS y cuál no; (2) en ambientes de múltiples operadores debe existir un acuerdo a nivel de servicio, también conocido como SLA (del inglés *Service Level Agreement*). En los últimos años se ha notado un gran crecimiento en el número de trabajos, proyectos y propuestas de estandarización [3GPP-Sharing] [Meddour2011] [Hultell2004] [Frisanco2008] [Beckman2005] que mencionan que en un futuro no muy lejano los operadores de telecomunicaciones no sólo compartirán infraestructura de redes, sino también servicios e información relativa a movilidad.

La información que puede intercambiase en escenarios con varios operadores es un aspecto crucial del servidor MIIS Global, ya que restringiendo información el usuario puede no recibir información detallada de las redes de acceso en una determinada zona, dejando así de hacer una buena transición. La principal ventaja del uso de este tipo de servidores MIIS es que ofrecen una completa y robusta visión de todas las redes de acceso pertenecientes a varios operadores sin almacenar ninguna información confidencial en un punto central de la red.

El algoritmo que describe cómo el usuario obtiene la información del servidor MIIS Global se ilustra en la Figura 3.10. Así, cuando un usuario móvil envía una solicitud de información, contacta directamente a su MIIS Zonal. En este caso, como la petición está relacionada con alguna red perteneciente a una

zona de otro operador, el MIIS Zonal reenvía la petición al servidor MIIS Local que la reenvía, a su vez, al MIIS Global. El MIIS Global del usuario envía la solicitud al MIIS Global del otro operador, que verifica si es un punto de acceso conocido y, si es así, el MIIS Global remoto contacta al MIIS Zonal de la red solicitada, obteniendo la información deseada por el usuario. Si el MIIS Global del usuario verifica que el punto de acceso detectado no pertenece a ningún operador, envía un mensaje de respuesta al usuario con contenido vacío.

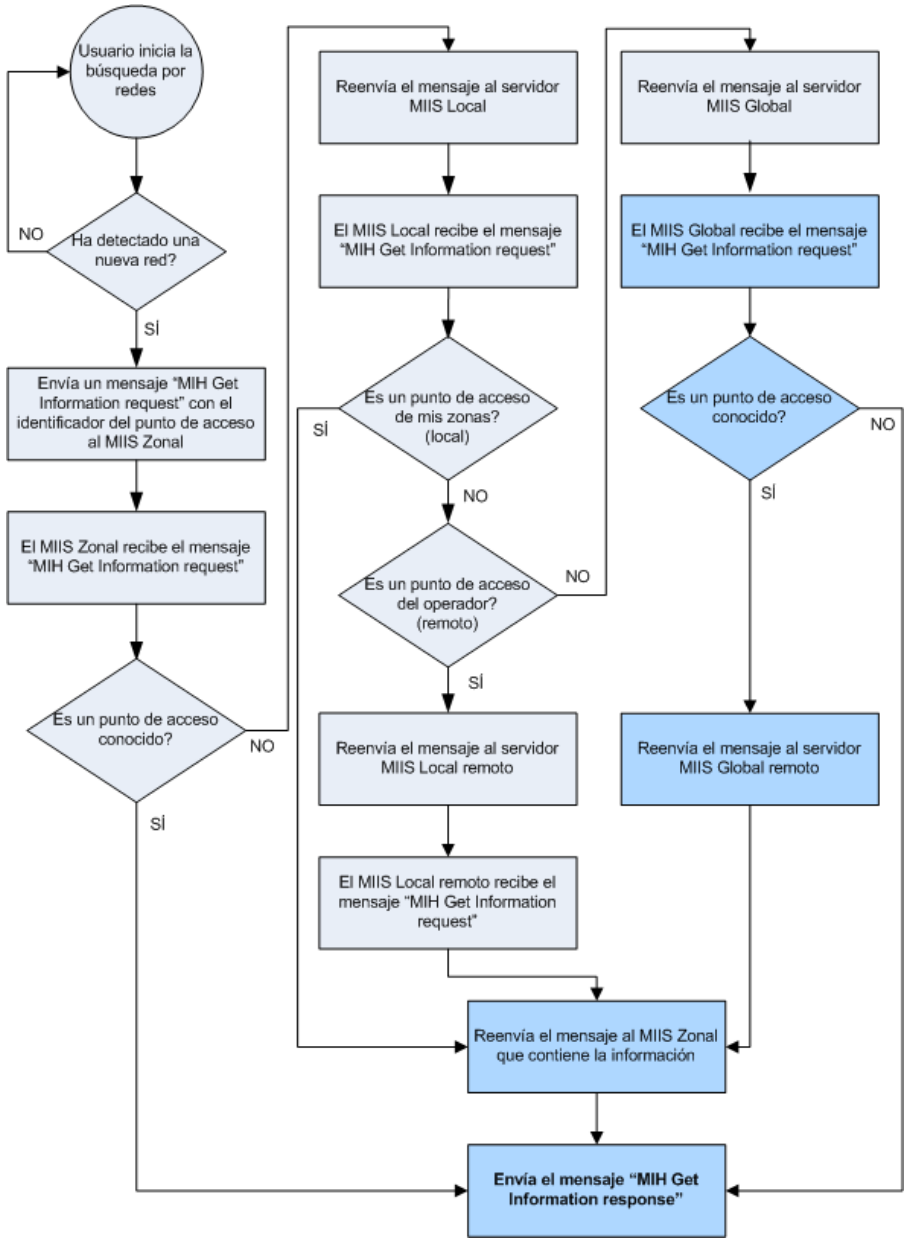

Figura 3.10: Algoritmo de funcionamiento del servidor MIIS Global.

En la Figura 3.11, se muestra un escenario con un servidor MIIS Global que gestiona la comunicación entre diferentes zonas de movilidad en un entorno con múltiples operadores. Puede observarse que el servidor MIIS Global está ubicado en Internet o en algún *backbone* común de los operadores. Su principal rol es actuar como intermediario entre la comunicación de dos o más operadores y permitir que un usuario móvil tenga una visión general de las redes en una determinada zona, aunque los puntos de acceso sean de operadores diferentes.

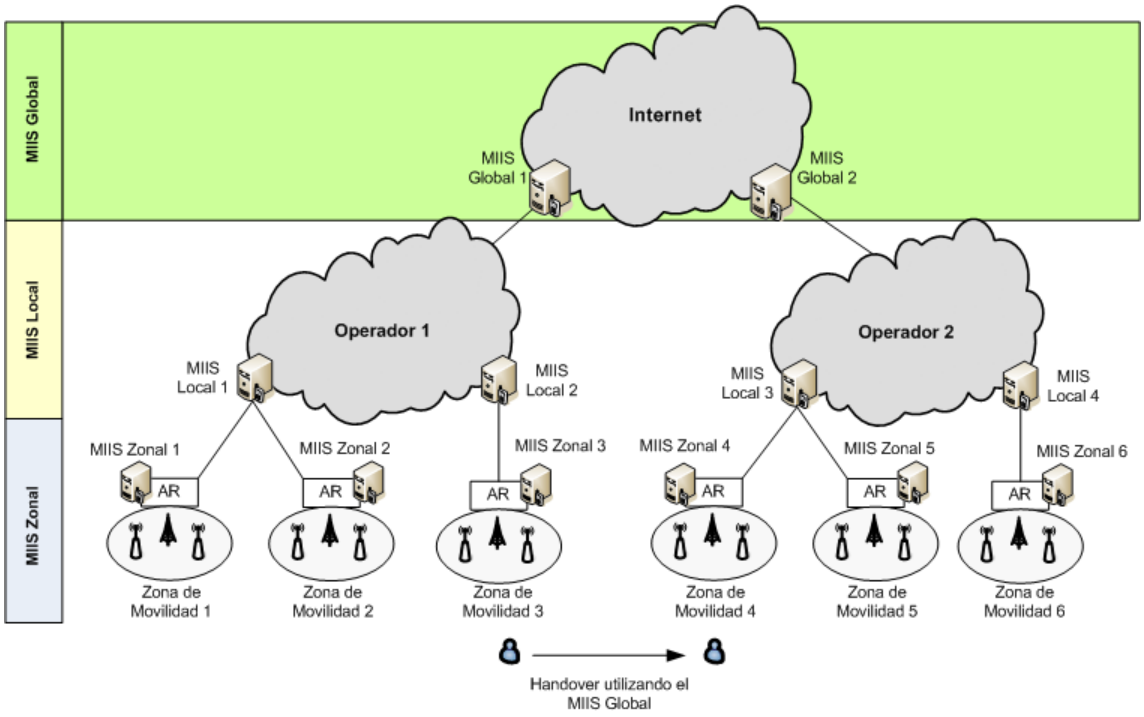

Figura 3.11: Ubicación física del servidor MIIS Global.

Como se ha comentado en la sección 4.2, tres son los requisitos para el despliegue de un servidor de información. Para el servidor MIIS Global tenemos las siguientes características:

1. **Ubicación física del servidor MIIS Global**: el servidor MIIS Global está ubicado físicamente en Internet o en algún backbone común de dos o más operadores. Comúnmente, el usuario móvil está de cuatro a diez saltos de

distancia del servidor MIIS Global.

2. **Información almacenada en el servidor MIIS**: dado que un servidor MIIS Global no almacena información detallada de las redes, en este tipo de servidor se almacena básicamente el identificador de las redes, la zona a la que pertenece cada punto de acceso y si la red del usuario tiene algún acuerdo de roaming con otros operadores.

3. **Periodicidad del envío de la información a los usuarios por parte del servidor MIIS**: la información almacenada en el servidor MIIS Global sólo se utiliza cuando un usuario quiere saber más información de un punto de acceso que está en una zona de otro operador.

3.5.1. Elementos de Información

En la Figura 3.12 se indican los elementos de información que puede contener un servidor de información MIIS Global. El servidor de información MIIS Global almacena prácticamente la misma información que el servidor MIIS Local, con excepción del nuevo elemento de información IE_Inter_Domain, que sirve para identificar con qué operadores la red actual tiene acuerdos de transición. Como se describe en el siguiente ítem, este elemento de información ha sido creado para identificar qué acuerdos de servicio hay entre los operadores.

Conviene reseñar que el estándar ofrece un elemento de información que permite identificar los acuerdos de transición que existan entre dos o más operadores: el IE_Roaming_Partners. Sin embargo, cuando se utiliza este elemento de información, dos operadores comparten la información de todas sus redes, no siendo posible especificar un conjunto de redes o puntos de acceso. Con el nuevo elemento de información, el IE_Inter_Domain, un operador puede especificar los puntos de acceso, las redes y las zonas de

movilidad que desea compartir con otros operadores.

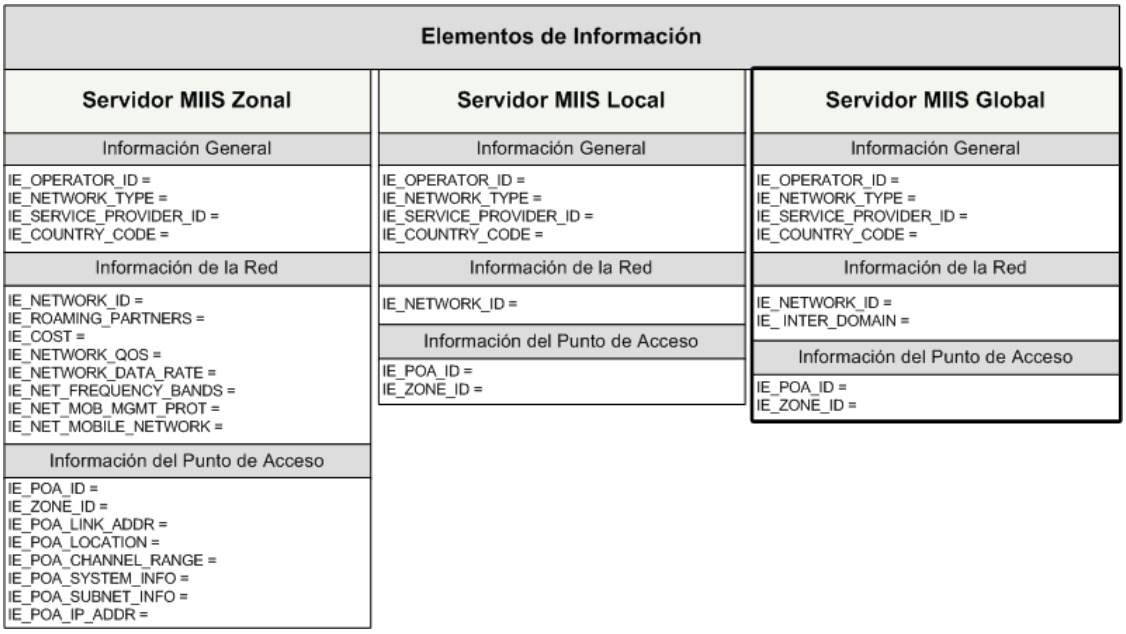

Figura 3.12: Elementos de Información de un servidor MIIS Global.

En Información General el servidor MIIS Global almacena información del operador como su nombre, su identificador, el código del país, etc. En Información de la Red se almacena el identificador de la red y el elemento *IE_Inter_Domain*. Por último, el grupo Información del Punto de Acceso contiene el identificador del punto de acceso *IE_PoA_ID* y el identificador de la zona del punto de acceso *IE_Zone_ID*.

3.5.2. Acuerdo de Nivel de Servicio entre Servidores MIIS Global

Como se ha comentado anteriormente, en la Internet móvil del futuro, se espera que los operadores colaboren entre sí y compartan tanto infraestructura de redes como información de movilidad. Para que haya esta colaboración se ha creado el elemento de información *IE_INTER_DOMAIN*. Este elemento de información se almacena únicamente en los servidores MIIS Global de cada operador. De esta forma, se introduce aquí el modelo de "acuerdo de nivel de servicio entre servidores MIIS Global", abreviadamente MSLA (del inglés *MIIS*

Service Level Agreement). El modelo MLSA especifica que cada MIIS Global negocia acuerdos de cooperación con otros MIIS Global para compartir información de movilidad.

Los servidores MIIS Global que utilicen el modelo MSLA y tengan un acuerdo de cooperación se conocen como servidores vecinos. Un servidor sólo acepta solicitudes de otros con los que mantiene acuerdos. De ahí que el usuario sólo puede obtener información adicional de un punto de acceso de otro operador si los dos servidores MIIS Global son vecinos.

La Tabla 3.1 ilustra la estructura de datos donde se especifica el acuerdo de servicio que deben tener los servidores MIIS Global para que se comuniquen y ofrezcan al usuario la posibilidad de hacer transición entre diferentes operadores.

Tipo de Datos	Proviene de	Definición
IE_INTER_DOMAIN	CHOICE (IE_ROAMING_PTNS, NULL)	Estructura que contiene una lista de los operadores que desean compartir recursos
IE_ROAMING_PTNS	LIST (OPERATOR_ID)	Una lista de acuerdos de transición
OPERATOR_ID	SEQUENCE (OP_NAME, LIST(MSLA))	Un tipo que representa el identificador del operador
OP_NAME	OCTECT_STRING	Un tipo que representa el nombre del operador
MSLA	SEQUENCE (IE_ZONE_ID)	Un tipo que representa los acuerdos MSLA
IE_ZONE_ID	OCTECT_STRING	Un tipo que representa el identificador de la zona

Tabla 3.1: Acuerdo de servicio entre servidores MIIS

El elemento de información *IE_Inter_Domain* permite que un punto de acceso tenga una lista de acuerdos de transición con otros puntos de acceso, zonas de movilidad u operadores. El *IE_Inter_Domain* es un conjunto de elementos *IE_Roaming_Ptns* (lista de acuerdos de *handover* basados en el identificador del operador *Operator_ID*). Éste se divide en dos campos: el nombre del operador y la lista de acuerdos MSLA. El campo MSLA representa los acuerdos entre los servidores MIIS Global y se compone de una secuencia o una lista de zonas de movilidad.

Con esta estructura se puede saber por ejemplo que el punto de acceso A de la zona de movilidad A del operador A tiene un acuerdo con la zona de movilidad B del operador B. Teniendo un acuerdo con la zona B, el usuario del punto de acceso A puede hacer *handover* para cualquier punto de acceso perteneciente a la zona B. Además, esta estructura tiene total flexibilidad ya que permite especificar acuerdos de servicio entre diferentes zonas de movilidad o integralmente entre operadores, al contrario del elemento de información *IE_Roaming_Partners* del estándar original.

3.5.3. Señalización

La Figura 3.13 muestra la comunicación que debe existir entre el usuario móvil y el servidor MIIS Global cuando el usuario está haciendo un *handover* entre dos puntos de acceso administrados por dos operadores diferentes. En esta comunicación el usuario envía el mensaje *MIH Get Information request* al punto de acceso que lo reenvía hacia al servidor MIIS Global. Este lo reenvía al servidor MIIS Zonal que tiene información del punto de acceso detectado. El MIIS Zonal responde a través del mensaje *MIH Get Information response*, que hace el camino inverso llegando al usuario final como *MIH Get Information* confirm.

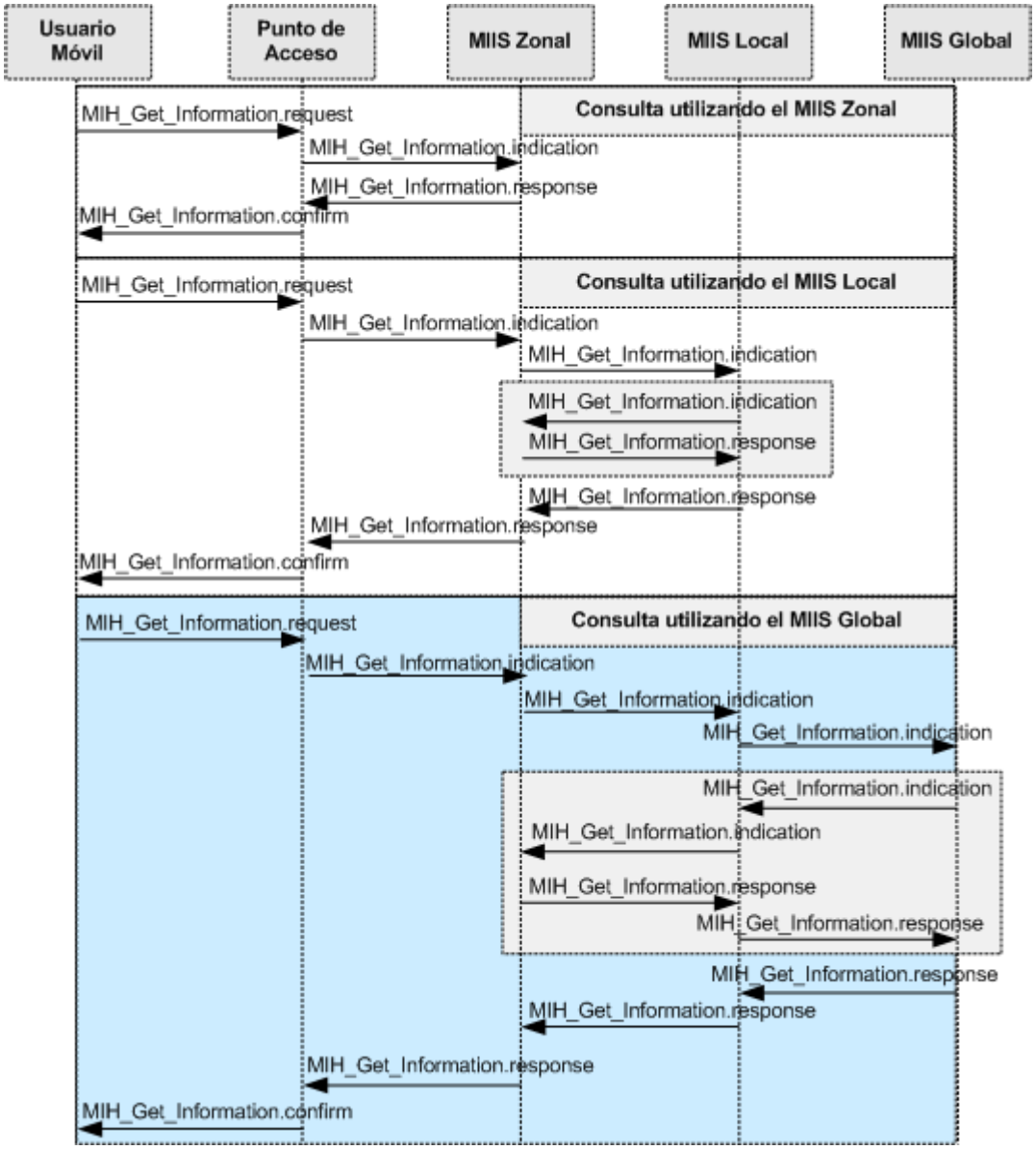

Figura 3.13: Comunicación entre el usuario y el MIIS Global.

La principal ventaja que tiene un servidor MIIS Global es permitir a un usuario móvil hacer una transición entre operadores diferentes, mejorando su experiencia móvil. El principal inconveniente es que el servidor MIIS Global no tendrá completa información de las redes a ofrecer al usuario móvil si, no hay cooperación entre los operadores.

La Tabla 3.2 resume las principales características de cada uno de los servidores MIIS propuestos en este trabajo. Respecto a la arquitectura jerárquica

de servidores MIIS cabe señalar que el uso de un determinado tipo de servidor depende de la infraestructura del operador de red (y de negocios y estrategias comerciales). Está previsto el despliegue de un sistema de información de movilidad como parte de la Internet Móvil del Futuro, lo que permitirá a los usuarios móviles desplazarse por diversas redes sin sufrir interrupción alguna en la comunicación.

Servidor MIIS	Arquitectura	Características	Información de los puntos de acceso	Señalización
Zonal	Centralizada. Acceso directo al servidor MIIS Zonal.	El más fácil de implementar. Un MIIS único por zona. No es escalable.	Información limitada. Sólo información de los puntos de acceso de la zona están disponibles.	El mejor rendimiento. Rápida respuesta al usuario
Local	Híbrido. El servidor MIIS puede reenviar la solicitud de información a un servidor en concreto.	Control de alto nivel sobre varios MIIS Zonal. Necesita un protocolo de comunicación entre los MIIS y actualizaciones con respecto a cada zona de movilidad. De plena confianza del dominio administrativo.	Medio. Puede reenviar la solicitud a otros MIIS que contienen la información del punto de acceso.	Tiene un tiempo de respuesta más largo que el MIIS Zonal, pero ofrece más opciones de puntos de acceso de diferentes zonas para que el usuario haga la transición.
Global	Totalmente distribuido. Puede contener información de múltiples operadores, en función de los acuerdos de servicios establecidos.	Apoyo a transiciones entre operadores. Requiere de acuerdos entre operadores de servicios y el protocolo de comunicación entre servidores MIIS.	Completa. El usuario puede obtener información de cientos o miles de puntos de acceso de varios operadores.	Como los MIIS Global actúan como un proxy para otros MIIS, presenta un buen desempeño de señalización, pero requiere actualización de la información entre los servidores MIIS Zonal, Local y Global.

Tabla 3.2: Comparativa de las características de los tipos de servidores MIIS

Utilizando esta arquitectura de comunicación cualquier usuario móvil podrá conocer a través de cualquier tecnología de red cuáles son los operadores, redes y puntos de acceso en su vecindad. Esta arquitectura proporciona al usuario

móvil una mejora significativa en el *handover* entre redes heterogéneas.

3.6. Síntesis del Capítulo

El principal objetivo de este capítulo ha sido especificar un sistema de información de movilidad con el objetivo de reducir el tiempo de descubrimiento de redes vecinas y mejorar la calidad de los *handovers* entre redes de distintas tecnologías y con diferentes operadores. El sistema propuesto considera la división de las redes de acceso en zonas geográficas de movilidad, clasificadas de forma jerárquica, y administradas por distintos tipos de servidores MIIS: MIIS Zonal, MIIS Local y MIIS Global.

También se ha visto una comparativa de las características de cada servidor MIIS propuesto, señalando sus propiedades y ventajas.

El sistema de información de movilidad forma parte de lo que se llama la Internet Móvil del Futuro donde los operadores de telecomunicaciones comparten infraestructura de redes y servicios y el usuario puede desplazarse por diversas redes de distintas tecnologías y de operadores diferentes.

4. SEGURIDAD EN EL ESTÁNDAR IEEE 802.21

4.1. Autenticación, Autorización, Auditoría y Calidad de Servicio entre Operadores

El modelo tradicional de telecomunicaciones donde el operador de redes móviles es el único propietario de todos los elementos de la red física y de las distintas capas de la red está cambiando. Esta tendencia, combinada con la creciente competencia, la rápida mercantilización de equipos de telecomunicaciones y la separación cada vez mayor de la red y de los servicios ofrecidos, presionan a los operadores a adoptar múltiples estrategias, con infraestructuras de red compartidas en las redes de acceso y también en el núcleo, surgiendo así un mecanismo más eficiente y sostenible respecto a los costes de la red.

En la Internet móvil del futuro se valora positivamente la posibilidad de que un usuario pueda itinerar entre operadores diferentes de forma totalmente transparente. Para ello, los operadores deben tener un acuerdo a nivel de servicio (*Service Level Agreement - SLA*) donde compartirán infraestructura, costes, beneficios y usuarios.

En este contexto resulta imprescindible la especificación de un mecanismo de seguridad para ambientes con múltiples operadores.

4.2. Identificación y Análisis de los Principales Mecanismos y Protocolos de Seguridad para Redes Móviles Heterogéneas

En cuanto al estado actual de los conocimientos científico-técnicos puede señalarse que apenas existe bibliografía sobre los mecanismos de seguridad en el proceso de obtención de la información de un servidor MIIS.

Uno de los primeros trabajos sobre el tema se publicó en la revista *IEEE Communications Magazine* en abril de 2008 [MPA2008]. El citado trabajo especifica un protocolo de seguridad conocido como "Pre-Autenticación Independiente del Medio" (MPA – *Media-Independent Pre-Authentication*) para *handovers* (transiciones) entre diferentes operadores.

Una versión más elaborada del trabajo anterior ha dado lugar a un draft [MPA2010] que todavía está en fase de borrador. Se espera una versión definitiva del mismo para finales del presente año. Los investigadores que llevan a cabo este estudio pertenecen a las empresas Telcordia Technologies (EEUU) y Toshiba Corporation (Japón) y a la Universidad de Columbia (EEUU).

También desde 2008 existe el Grupo de Trabajo IEEE 802.21a [IEEE2009] que especifica extensiones de seguridad para el protocolo IEEE 802.21. En 2009 se publicó las "*Call for Proposals*" y en 2010 empezaron a escribir el documento oficial, que será el futuro estándar IEEE 802.21a.

Aparte del IEEE 802.21a, en [Rodri2009] los autores trabajan en la integración de una arquitectura IMS (*IP Multimedia Subsystem*) + MPA. Con este *framework* se habilita movilidad en entornos IMS y se garantiza una transición segura al usuario móvil.

En [Li2010] los autores especifican un mecanismo de seguridad para un servidor MIIS en redes heterogéneas en el que la clave es el establecimiento de un túnel seguro de comunicación entre el usuario móvil y el servidor MIIS.

[Lun2010] propone una versión mejorada del protocolo MPA. Según el autor, el e-MPA (*Enhanced-MPA*) previene la pérdida de paquetes en la ejecución del *handover*.

[Ohba2010] propone el uso del protocolo EAP (*Extensible Authentication Protocol*) como protocolo de autenticación donde el usuario móvil puede autenticarse con cualquier red candidata antes de que se conecte propiamente a ella. Es decir, el usuario hace una pre-autenticación, disminuyendo el tiempo final del *handover*.

Por último, [Marin2010] describe una arquitectura que reduce el retardo en el proceso de re-autenticación utilizando el protocolo EAP-FRM.

4.3. Estudio Detallado del Protocolo IEEE 802.21a

Como se puede ver en la Figura 4.1, el protocolo MPA especifica tres grandes entidades de comunicación: un *router* de acceso (AR), un agente de autenticación (AA) y un agente de configuración (CA).

Para que el usuario móvil establezca una comunicación segura y pueda hacer un *handover* entre diferentes operadores son necesarias tres etapas:

1. Pre-Autenticación: en esta etapa se establece una asociación segura entre el usuario móvil (MN) y alguna red candidata (CTN - Candidate Network) a través del agente de autenticación (AA).

2. Pre-Configuración: en la segunda etapa el usuario obtiene configuración

IP (ej: el protocolo de distribución de configuraciones de red DHCP) y otras informaciones de la CTN, así como establece un Proactive Handover Tunnel (PHT) entre el MN y el AR de la CTN.

3. Handover Proactivo Seguro: a través del túnel PHT se envían y reciben mensajes IP. Una vez realizada la comunicación se borra el túnel PHT inmediatamente después de asociarse a la CTN.

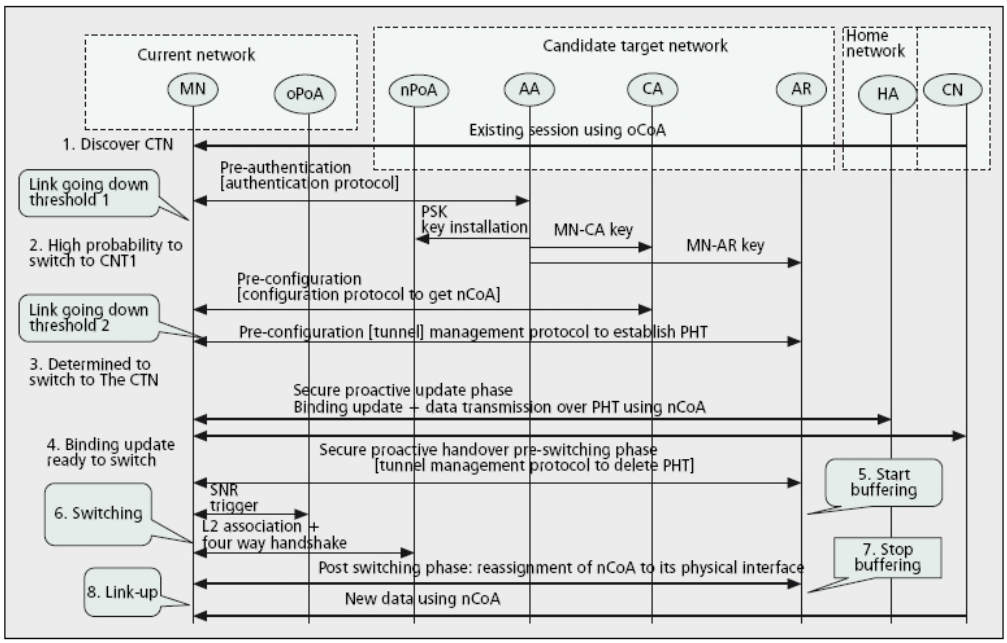

Figura 4.1. Señalización del protocolo MPA.

El futuro estándar IEEE 802.21a será sin duda el referente en el área de seguridad para handovers entre medios heterogéneos.

5. ESPECIFICACIÓN DE UN MECANISMO DE SEGURIDAD PARA REDES MÓVILES HETEROGÉNEAS

Para proporcionar seguridad en el proceso de descubrimiento de información utilizando el servidor MIIS se necesita un Authentication Server (AS) en cada operador. Se ha decidido representar cada AS como una entidad independiente debido a la modularidad que proporciona esta alternativa. Esta decisión tiene la ventaja de no sobrecargar el servidor MIIS ya que sólo se necesita proporcionar la autenticación en el operador que provee el servicio.

Para que los *handovers* se realicen correctamente entre redes heterogéneas, cada Mobile Node (MN) tiene que suscribirse al MIIS con la seguridad proporcionada por el AS. Cada AS mantiene una entrada para el MN registrado. Después de que un MN se autentica, debe contactar con el servidor MIIS para obtener información sobre las redes vecinas.

Proceso de comunicación entre el MN y el servidor MIIS:

1. El MN se comunica con el operador destino a través del LMIIS y le devuelve dos direcciones: la dirección del AS de este operador y la dirección del ZMIIS, al que pertenece el PoA detectado. (Esta fase nos proporciona información del PoA que detecta el MN).

2. El AS de este operador envía la clave a esta nueva zona (ZMIIS)

3. El MN se autentica con el AS del operador destino.

4. El MN se comunica con el ZMIIS del PoA al que se conecta.

Consideraciones:

Siempre que se pasa de una zona a otra es necesaria la autenticación, aunque las zonas pertenezcan al mismo operador. Cada zona tiene asociada una clave de acceso única.

A continuación se expone el funcionamiento para un escenario ejemplo.

Se representa una estructura jerárquica de servidores MIIS, en la que se observan 3 niveles de información: el núcleo (llamado *backbone*), el nivel de operadores y el nivel de las zonas de movilidad.

En este escenario tenemos un *backbone* con información de 2 operadores. Estos 2 operadores tienen 2 zonas por operador, en los que se ubican sus correspondientes AS y sus MIIS Locales. Se dispone, por tanto, de un total de 4 zonas de movilidad.

En cada zona disponemos de 4 PoAs (*Point of Attachment*) Wi-Fi y 1 PoA Wi-Max. Cada una de las zonas dispone de un *Access Router* (AR). El MN realiza un *handover* al desplazarse desde la zona 2 hasta la zona 3 como se muestra en la Figura 5.1.

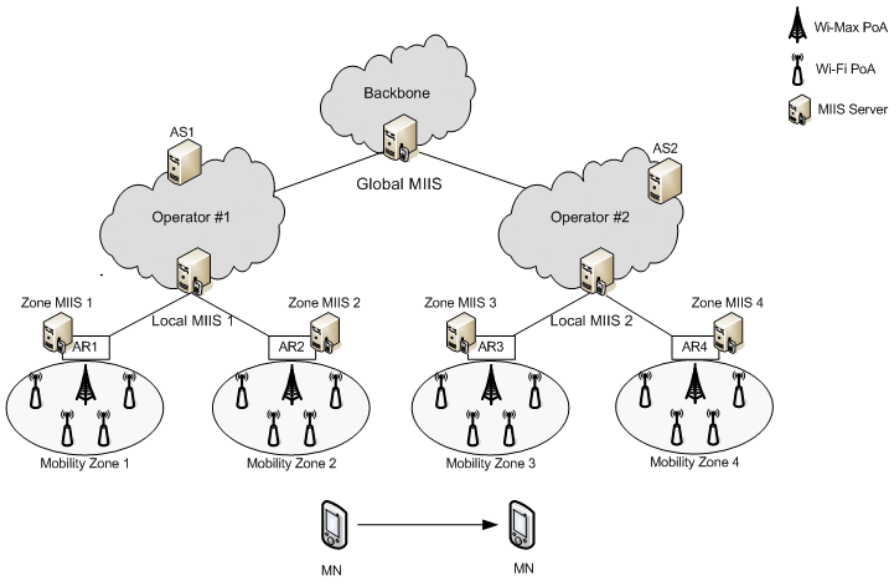

Figura 5.1. Ubicación de los MIIS en el escenario ejemplo.

El diagrama de flujo del escenario ejemplo se muestra en la Figura 5.2. Se realiza un *handover* entre zonas de distintos operadores. La autenticación siempre es necesaria entre zonas.

El MN que se desplaza desde la zona 2 a la zona 3 detecta un nuevo PoA de una red Wi-Fi. El MN no tiene información de esta nueva red, por lo que envía un mensaje de solicitud de información al operador 2 a fin de obtener más información sobre la zona del PoA detectado. Este mensaje *MIH_Get_Information_Request* contiene el ID del PoA detectado.

El MIIS Local (LMIIS2) del operador 2 responde con un mensaje *MIH_Get_Information_Response* que incluye la dirección IP del AS2 y del ZMIIS3. Realizada esta fase, el MN ya puede autenticarse con el AS2 del operador 2. En este proceso AS2 envía una clave MN-AS2 al ZMIIS3.

Una vez autenticado, el MN se comunica con el servidor MIIS de la zona 3 (ZMIIS3) enviando un mensaje *MIH_Get_Information_Request*. Este mensaje contiene el PoA ID detectado y la clave asociada a este MN.

Cuando el ZMIIS3 recibe este mensaje, comprueba que la clave del mensaje corresponde a la MN-AS2. Si esto es correcto, envía un mensaje de respuesta *MIH_Get_Information_Response* con la información del PoA detectado. En caso contrario, se deniega al MN la conexión a esta zona.

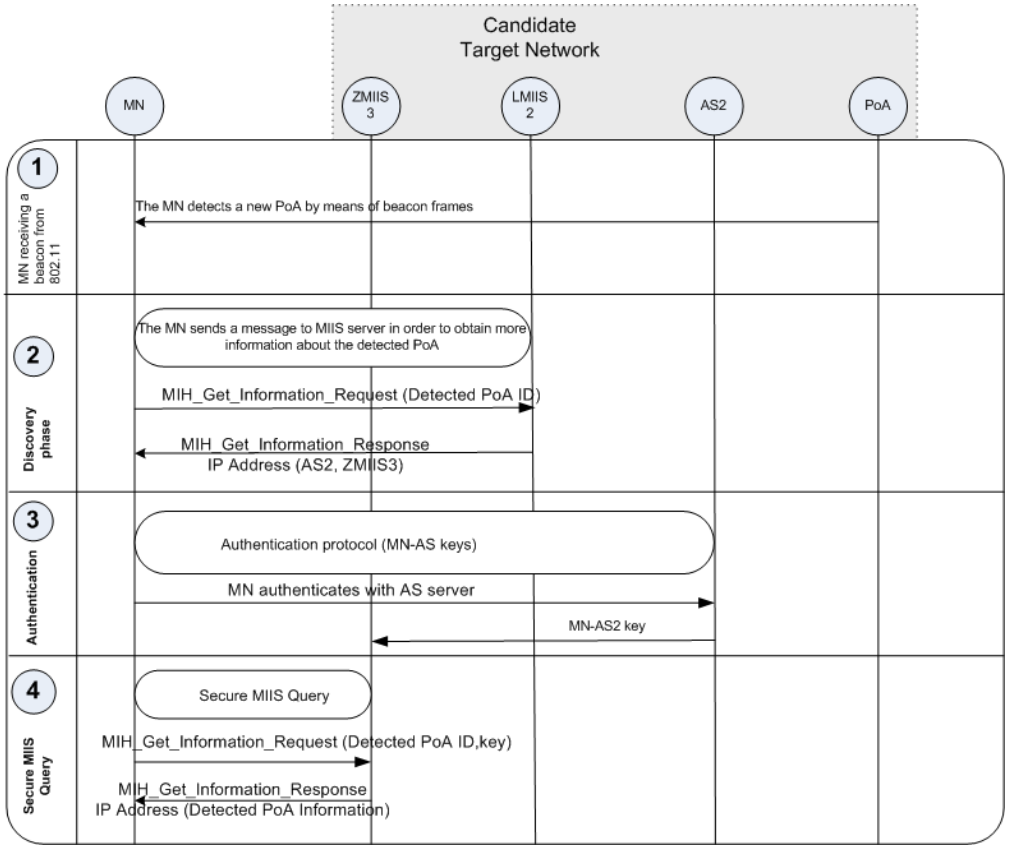

Figura 5.2. Diagrama de Flujo en el escenario ejemplo.

6. CONCLUSIONES Y TRABAJO FUTURO

Este trabajo aborda la problemática de la seguridad de una arquitectura de servidores de información en redes heterogéneas incluyendo redes Wi-Fi, Wi-Max y las redes celulares 3G.

En primer lugar se ha analizado la necesidad de tener un servidor de información en un ambiente compuesto por varias redes pertenecientes a diferentes operadores.

En segundo lugar se ha hecho un detallado análisis del estándar IEEE 802.21 que proporciona inteligencia de capa de enlace y otra información de red relacionada con las capas superiores para optimizar la transición entre redes heterogéneas cuyo objetivo principal es mejorar la experiencia del usuario y facilitar la transición entre distintas redes de comunicación.

A continuación se han analizado los trabajos más representativos relativos al citado estándar, entre los que se incluyen la especificación de una arquitectura MIIS jerárquica.

Seguidamente se han revisado los trabajos de seguridad. De la escasa literatura encontrada destaca el protocolo MPA, llamado a convertirse próximamente en estándar.

Finalmente, se propone una arquitectura segura y jerárquica de servidores MIIS en la que se distinguen dos tipos de servidores de información, uno local que atiende solamente a un operador y el otro global que atiende a varios operadores y redes. Además, se ha hecho una propuesta de comunicación entre varios servidores de información considerando sus posibles ubicaciones físicas

dentro de una gran red con múltiples redes y múltiples operadores.

6.1. Trabajo Futuro

Como trabajo futuro, y que ya estamos haciendo es concretar algunos escenarios para certificar la validez de nuestra propuesta de especificación de una arquitectura de un servidor de información incluyendo su funcionamiento, sus principales características, sus elementos de información y su modelo de comunicación con otras entidades de la red.

Como trabajo más inmediato cabe señalar la elección del entorno de simulación pues del estudio preliminar realizado no es una elección trivial.

6.2. Divulgación de Resultados

El presente trabajo ha dado lugar a las siguientes publicaciones internacionales:

[Buiati_ICIT2011] F. Buiati, I. Saadat, D. Rupérez Cañas, L. J. García Villalba: "**IEEE 802.21 Information Service: Features and Implementation Issues**", The 5th International Conference on Information Technology (ICIT 2011), May 2011, Jordan.

[Ismail2011] I. Saadat, F. Buiati, D. Rupérez Cañas, L. J. García Villalba, "**Overview of IEEE 802.21 Security Issues for MIH Networks**", The 5th International Conference on Information Technology (ICIT 2011), May 2011, Jordan.

REFERENCIAS

[3GPP] 3rd Generation Partnership Project, "Technical Specification Group Services and Systems Aspects; Network Architecture", 3GPP, March 2006.

[3GPP-Sharing] 3GPP: 23.851 Technical Specification Group Services and System Aspects; Network sharing; Architecture and Functional Description; (Release 6), 2004.

[802.11] IEEE Std 802.11-1997 Information Technology – Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks – specific Requirements – part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-1997, 1997, pp. i-445.

[802.16] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands. IEEE 802.16e-2005.

[802.21] IEEE 802.21, Standard, Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services", January 2009.

[Baek2008] Baek, D. Kim, Y. Suh, E. Hwang, and Y. Chung, "Network-Initiated Handover Based on IEEE 802.21 Framework for QoS Service Continuity in UMTS/802.16e Networks", Proceedings of the IEEE VTC 2008, May 2008.

[Beckman2005] C. Beckman, G. Smith, Shared networks: making wireless communication affordable, IEEE Wireless Communications (2005) 78–85.

[BT-FON] Comunidad BT-FON, http://www.btfon.com

[Buiati_FGCN2011] F. Buiati, L. J. G. Villalba, D. R. Cañas, and T. Kim, "Improving the Wi-Fi Channel Scanning Using a Decentralized IEEE 802.21 Information Service," in Multimedia, Computer Graphics and Broadcasting, vol. 263, Springer Berlin Heidelberg, 2011, pp. 290–294.

[Buiati_ICIT2011] F. Buiati, I. Saadat, D. Rupérez Cañas, L. J. García Villalba, "IEEE 802.21 Information Service: Features and Implementation Issues", The 5th International Conference on Information Technology (ICIT 2011), May 2011, Jordan.

[Buiati2010] Fábio Buiati, Luis Javier García Villalba, Daniel Corujo, João Soares, Susana Sargento, Rui L. Aguiar, "Hierarchical Neighbor Discovery Scheme for Handover Optimization", IEEE Communication Letters, ISSN 1089-7798, vol.14, no.11, pp.1020-1022, November 2010.

[Buiati2011] F. Buiati, L. J. G. Villalba, D. Corujo, S. Sargento, and R. L. Aguiar, "IEEE 802.21 Information services deployment for heterogeneous mobile environments", Communications, IET, vol. 5, no. 18, pp. 2721 –2729, 2011.

[Cacace2006] F. Cacace and L. Vollero, "Managing Mobility and Adaptation in Upcoming 802.21 Enabled Devices", Proc. 4th Int'l. Wksp. Wireless Mobile Apps. and Services on WLAN Hotspots, 2006.

[Christakos2009] Christakos, C.; Izquierdo, A.; Rouil, R.; Golmie, N., "Using the Media Independent Information Service to Support Mobile Authentication in Fast Mobile IPv6," Wireless Communications and Networking Conference, 2007. WCNC 2009, March 2009.

[FastMIP] R. Koodli, editor. "Mobile IPv6 Fast Handovers". IETF RFC 5268, Junio 2008.

[Floroiu2007] J. Floroiu, M. Corici, Byoung-Joon Lee, S. Lee, S.Arbanowski, and T. Magedanz, "A Vertical Handover Architecture for End-to-End Service Optimization", 16th IST Mobile and Wireless Communications Summit, 2007, July 2007.

[Frisanco2008] T. Frisanco et al., "Infrastructure Sharing and Shared Operations for Mobile Network Operators – From a Deployment and Operations View", in: Proceeding on International ICOIN Conference, 2008, pp.1–5.

[Giaffreda2007] R. Giaffreda, K. Pentikousis, E. Hepworth, R. Aguero, A. Galis, "An Information Service Infrastructure for Ambient Networks", Proceedings of the 25th IASTED International Multi-Conference Paralell and Distributed Computing and Networks, February 2007.

[Hultell2004] J. Hultell, K. Johansson, J. Markendahl, “Business models and resource management for shared wireless networks”, in: IEEE Vehicular Technology Conference, 2004.

[Intel] Kapil Sood, Emily H. Qi, Vivek G. Gupta, “Seamless Platform Mobility across Wireless Networks”, Technology@Intel Magazine, September 2005.

[Ismail2011] I. Saadat, F. Buiati, D. Rupérez Cañas, L. J. García Villalba, “Overview of IEEE 802.21 Security Issues for MIH Networks”, The 5th International Conference on Information Technology (ICIT 2011), May 2011, Jordan.

[Khan2011] Khan, M.Q.; Andresen, S.H., "An Intelligent Scan Mechanism for 802.11 Networks by Using Media Independent Information Server (MIIS)", Advanced Information Networking and Applications (WAINA), 2011 Conference on IEEE Workshops of International, pp.221-225, 22-25 March 2011.

[Kim2010] Y. Kim et al., “An enhanced information server for seamless vertical handover in IEEE 802.21 MIH networks”, Comput. Netw. (2010), doi:10.1016/j.comnet.2010.08.005.

[Kutscher2006] Dirk Kutscher and Jorg Ott, “Service Maps for Heterogeneous Network Environments”, Proceedings of the 7th International Conference on Mobile Data Management (MDM 06).

[Kutscher2006a] Dirk Kutscher and Jorg Ott., “Enhancing User Mobility with Network Service Maps”, In Proceedings of TERENA Networking Conference 2006, May 2006.

[Lampropoulos2008] G. Lampropoulos, A. Salkintzis, N. Passas, “Media-Independent Handover for Seamless Service Provision in Heterogeneous Networks”, IEEE Communications Magazine, January 2008.

[Lampropoulos2010] George Lampropoulos, Charalabos Skianis, Pedro Neves, “Optimized fusion of heterogeneous wireless networks based on media-independent handover operations”, IEEE Wireless Communications Magazine, 2010.

[Lim2009] W. S. Lim, D. W. Kim, Y. J. Suh and J. J. Won, “Implementation and Performance Study of IEEE 802.21 in Integrated IEEE 802.11/802.16e Networks”, Computer Communications, Volume 32, Issue 1, Pages 134-143, January

2009.

[Liu2009] H. Liu, C. Maciocco, V. Kesavan and A. Low, “IEEE 802.21 Assisted Seamless and Energy Efficient Handovers in Mixed Networks”, Mobile Wireless Middleware, Operating Systems, and Applications, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 7. ISBN 978-3-642-01801-5. Springer Berlin Heidelberg, 2009.

[Liu2009_2] Huaiyu Liu; Maciocco, C.; Kesavan, V.; Low, A.L.Y., "Energy efficient network selection and seamless handovers in Mixed Networks", World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a , vol., no., pp.1-9, 15-19 June 2009.

[Meddour2011] D.-E. Meddour et al., “On the role of infrastructure sharing for mobile network operators in emerging markets”, Comput. Netw. (2011), doi:10.1016/j.comnet.2011.01.023.

[MIP] B. Patil, P. Roberts and C. E. Perkins, “IP Mobility Support for IPv4”, in RFC 3344. IETF, August 2002.

[MPA2008] A. Dutta et al, ”Media-Independent Pre-Authentication Supporting Secure Interdomain Handover Optimization”, IEEE Wireless Communications, April 2008.

[MPA2010] A. Dutta et al, “Media-Independent Pre-Authentication Supporting Secure Interdomain Handover Optimization”. Draft http://tools.ietf.org/html/draft-irtf-mobopts-mpa-framework-08 (última actualización: Septiembre 2010).

[IEEE2009] Y. Ohba et al, "Standard for Local and Metropolitan Area Networks: Media Independent Handover (MIH) Services - Amendment for Security Extensions to Media Independent Handover Services and Protocol” (in progress).

[Lun2010] Lun-Huo Yeh, “An Enhanced Media-Independent Pre-Authentication Framework for Preventing Packet Loss”. Proceedings of the Second International Conference on Communications Software and Networks (ISBN: 978-1-4244-5726-7), pp. 284-288, 2010.

[Li2010] Li et al, “SAM: Secure Access of Media Independent Information Service with User Anonymity”. EURASIP Journal on Wireless Communications and Networking, Vol. 2010. http://www.hindawi.com/journals/wcn/2010/249169/.

[Rodri2009] Carlos Rodrigues, Carlos Rabadão and António Pereira, "802.21-MPA-IMS Architecture", in Proceedings of the Fourth International Conference on Systems and Networks Communications (ISBN: 978-1-4244-4772-5), pp. 94-99, 2009.

[Ohba2010] Ohba et al, "Extensible Authentication Protocol (EAP) Early Authentication Problem Statement". RFC 5836, April 2010.

[Marin2010] Rafael Marín Lopez, Antonio Fernando Gomez, Fernando Bernal Hidalgo and Fernando Periñíguez, "Architecture for Fast EAP Re-authentication based on a new EAP method (EAP-FRM) working on standalone mode", Disponible en: http://tools.ietf.org/html/draft-marin-eap-frm-fastreauth-02, 2010.

[Mussabir2007] Q. Mussabbir, W. Yao, Z. Niu, and X. Fu, "Optimized FMIPv6 Using IEEE 802.21 MIH Services in Vehicular Networks", IEEE Transactions on Vehicular Technology, pp. 3397–3407, November 2007.

[Neves2011] Pedro Neves, João Soares, Susana Sargento, Hugo Pires, Francisco Pontes, "Context-aware media independent information server for optimized seamless handover procedures", Computer Networks 2011.

[Oliva2008] De La Oliva, A.; Banchs, A.; Soto, I.; Melia, T.; Vidal, A., "An overview of IEEE 802.21: media-independent handover services" IEEE Wireless Communications, vol.15, no.4, pp.96-103, Aug. 2008.

[Pentikousis2007] Pentikousis, K.; Aguero, R.; Giaffreda, R.; Galis, A.; Hepworth, E., "Information Management for Dynamic Networks," International Multi-Conference on Computing in the Global Information Technology, 2007. ICCGI 2007, pp.43, 4-9 March 2007.

[Pontes2008] Pontes, A.; dos Passos Silva, D.; Jailton, J.; Rodrigues, O.; Dias, K.L., "Handover management in integrated WLAN and mobile WiMAX networks," Wireless Communications, IEEE, vol.15, no.5, pp.86-95, October 2008.

[RFC791] J. Postel. 'Internet Protocol', RFC 791. Septiembre 1981.

[Seol2007] J-H. Seol and J-M. Chung, "IEEE 802.21 MIH based Handover for Next Generation Mobile Communication Systems", Proceedings of 4th International Conference on Innovations in Information Technology, Innovations '07, Dubai, United Arab Emirates, November 2007.

[Taniuchi2009] K. Taniuchi, Y.Ohba, S. Das, M. Tauil, Y-H Chang, A.Dutta, D. Baker, M. Yajnik, D. Famolari, "IEEE 802.21: Media Independent Handover: Features, Applicability, Realization", IEEE Communications Magazine, January 2009.

[Vogueler2011] Karel De Vogeleer, Selim Ickin, David Erman, "A decentralized Information Service for IEEE 802.21 - Media Independent Handover (MIH)", IEEE Groups, 2011.

[Wu2006] M. Wu, Y. Chen, T. Chung and C. Hsu, "A Profile-Based Network Selection with MIH Information Service", Proc. of ICS'06, Samos Island, Greece, August/September 2006.

[Ying2008] W. Ying, Z. Yun, Y. Jun and Z. Ping, "An Enhanced Media Independent Handover Framework for Heterogeneous Networks", Proceedings of the IEEE Vehicular Technology Conference, pp.2306- 2310, May 2008.

[Yoo2008] Yoo, S., Cypher, D., Golmie, N., "Timely Effective Handover Mechanism in Heterogeneous Wireless Networks", In Proceedings of the Springer Wireless Personal Communications, 2008.

Title: IEEE 802.21 Information Service: Features and Implementation Issues

Author(s) name(s): Fábio Buiati, Ismail Saadat, Delfín Rupérez Cañas, Luis Javier García Villalba

Affiliation: Universidad Complutense de Madrid (UCM), Spain

Postal address:
Grupo de Análisis, Seguridad y Sistemas (GASS)
Departamento de Ingeniería del Software e Inteligencia Artificial (DISIA)
Facultad de Informática, Despacho 431
Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n
Ciudad Universitaria, 28040 Madrid, Spain

Phone number: +34 91.394.76.38

Fax number: +34 91.394.75.47

E-mail(s): {fabio, saadat, delfinrc, javiergv}@fdi.ucm.es

URL: http://gass.ucm.es/en/

Topic of the paper: Computer Networks & Communications

Title: IEEE 802.21 Information Service: Features and Implementation Issues

Abstract: The next generation of wireless networks terminals is expected to support multiple wireless radio access networks as Bluetooth, Wi-Fi, Wi-Max and UMTS in which users can maintain the connection when they switch from one network to another, in seamlessly manner. Supporting this type of handover in heterogeneous networks requires several constraints to be considered such as radio signal strength, coverage, security, QoS, user policies, cost, etc. In order to store information from several networks and operators, the new IEEE 802.21 standard specifies a media independent information service that supports various information elements providing network information within a geographical area, focusing on optimization of the handover process. This article presents a general approach towards Information Service management infrastructure in a heterogeneous mobile environment addressing the main features, security and implementation issues.

***Index Terms* — Mobility, IEEE 802.21, Heterogeneous Networks, Media Independent Handover, Inter-Domain, Service Discovery.**

IEEE 802.21 Information Service: Features and Implementation Issues

Fábio Buiati, Ismail Saadat, Delfín Rupérez Cañas, Luis Javier García Villalba

Abstract - **The next generation of wireless networks terminals is expected to support multiple wireless radio access networks as Bluetooth, Wi-Fi, Wi-Max and UMTS in which users can maintain the connection when they switch from one network to another, in seamlessly manner. Supporting this type of handover in heterogeneous networks requires several constraints to be considered such as radio signal strength, coverage, security, QoS, user policies, cost, etc. In order to store information from several networks and operators, the new IEEE 802.21 standard specifies a media independent information service that supports various information elements providing network information within a geographical area, focusing on optimization of the handover process. This article presents a general approach towards Information Service management infrastructure in a heterogeneous mobile environment addressing the main features, security and implementation issues.**

Index Terms — **Mobility, IEEE 802.21, Heterogeneous Networks, Media Independent Handover, inter-domain, service discovery, security.**

I. INTRODUCTION

WITH the proliferation of Wi-Fi (802.11) hotspots, the advent of Wi-Max (802.16) networks and the global reach of 3G mobile wireless services, the possibility of ubiquitous mobility for data transport is both a reality and a challenge. To make use of the available networks the mobile node (MN) will need to be equipped with several radio interfaces enabling them to associate with different networks from distinct operators in the future mobile Internet.

In this heterogeneous wireless environment, seamless handover is very important in order to minimizing aspects as data lost, low control overhead and transfer delay duration. In the literature [1], seamless handover is a type of handover in which service continuity and disruption time must be minimal. The handover can occur either between access points that use the same wireless technology (horizontal handover) or among two different points of attachment (PoA) belonging of different link layers technology (vertical handover). In such cases, the most important requirement is to provide the MN with sufficient information about neighbor networks to make an accurate handover decision.

In traditional (horizontal) handover, such as between cellular networks, the handover decision is based mainly on relative signal strength (RSS) information in the border region of two cells, as an indicator for service availability from a PoA. However, traditional RSS comparisons are not sufficient to make a vertical handover decision, as they do not take into account the various attachment options for the MN. This is because in heterogeneous network environments more parameters and information will be needed to make an accurate vertical handover decision. Besides RSS handover decision criteria, several other parameters such as current network utilization, expected throughput, cost per use, QoS supported, PoA geographical position and security are important.

In this way, the network information discovery phase is highly critical. To accomplish it, MN must be able to discover what types of network connectivity are accessible to them. Essentially, there are three basic alternatives to obtain network information: (1) the MN is provided with manually static information about geographical networks by means of a configuration file; (2) the MN listens to network "service advertisements" (e.g., 802.11 beacon frames and DCD 802.16 frames) to learn the accessible offered network services and (3) the mobile node can consult a network information entity, which can store information from several networks and operators. In this work, we will demonstrate the main benefit of using such network information discovery technique.

To assist seamless handover between networks belonging to same or different technologies, a network information service (IS) may be used. The main goal of IS usage is to allow the MN to acquire a global view of all heterogeneous networks information in the area before connectivity loss is experienced, hence improving the handover decision and mobile user experience.

At the forefront of network IS specification, the IEEE 802.21 [2] standard group is currently working on the standardization of a media independent information service (MIIS) that provides capability for obtaining information about lower layers such as security, neighbor maps, QoS and cost, as well as information about available high layer services such IP configuration methods and Internet connectivity. Moreover, the MIIS offers a set of information elements (IEs) containing different groups of mobility services that could be retrieved from different link layers technologies. Usually, these IEs are intended to provide mostly static information such as channel information, geographic position and security. Dynamic information such as pricing, current available resource level and current network utilization should be obtained directly from the interaction with the access network.

The MIIS must allow the information to be accessed from any single network, related not only to the technology to which the MN is currently attached, but to the surrounding available technologies. By way of example, a MN using its Wi-Fi interface should be able to access information from all others IEEE 802 based networks as well as 3G cellular networks.

Under those circumstances, the IEs can be stored on a single centralized MIIS server [2] or distributed among several MIIS servers in a decentralized way [3]. In the interaction between an MIIS server and a MN, a series of steps are required before information is able to be delivered back to the MN. Initially, the MIIS server must be discovered by the MN, probably using layer 2 or layer 3 based mechanisms depending of its location in the network. Subsequently, a secure association may be established in order to ensure the validity of the data communication. Finally, the MN and the MIIS server can exchange information using a transport protocol which works whether MIIS server is on the same subnet or deep in the network.

The rest of this article is organized as follows. Initially, we briefly present the main network information discovery techniques by which the MN can discover a service or a network. After that, the main entities and services of the emerging IEEE 802.21 standard are showed focusing on the MIIS domain. Then we introduce a mobility information structure, including its elements and data representation mechanism. Subsequently, we discuss the MIIS server discovery procedures as issues associated with the transport and security of IEEE 802.21 messages through an operation signaling flow example. Next, we present the main security and implementation issues. As a final point, we conclude this work with some final considerations and open topics for future works.

II. NETWORK INFORMATION DISCOVERY

In order for a MN to obtain connection to a PoA such as Wi-Fi access point or Wi-Max and 3G base stations, it needs to first discover the services offered by the PoAs in the vicinity. Typically, the available information about candidate networks is rather minimal but sufficient for a MN to learn some parameters before choosing and joining the network. In this section, we describe the main network information discovery techniques.

Statically Preconfigured Information

The MN is provided with manually preconfigured static information about geographical networks by means of a configuration file. One advantage of using such a technique is that no messages are exchanged, therefore no traffic is generated to the network, and hence overhead is reduced. On the other hand the method clearly presents no benefits and is not scalable. By using such approach the MN risks not to have updated network information ever.

Network Service Advertisement

Some technologies such Wi-Fi and Wi-Max wireless networks already have an existing means of detecting a list of neighborhood networks within the vicinity. Typically, the MN turns on its wireless interface and can listen to network “service advertisements” messages (e.g., 802.11 beacon frames, IEEE 802.16 DCD) and attempt to connect to PoA. Usually, a service advertisement message contains just enough information which is necessary for a client station to learn about the parameters of the PoA before joining to the network.

The benefit of using this network discovery technique is that the network information comes within the periodic broadcast message saving the MN the task of consulting any entity of the network. Conversely, scanning multiple channels on different technologies is very expensive or consuming both in terms of time and battery-level. In addition, the MN must be a network in range to receive the advertisements messages and the operator must be willing to distribute network information.

Accessing a MIIS Server

In the last network information discovery technique, the mobile node can consult a MIIS server, which stores information from several access networks and operators. To access this information, the MN must perform some steps before obtaining the desired information. It may require link-layer supports, transport protocol capability and security considerations. The main advantage of using such a technique is that the MN may have a complete and consistent view of the whole network. In addition, this approach allows MN mobility over several networks and operators. In this work, we will use this approach to demonstrate the benefits of use MIIS server technique in a heterogeneous mobile network environment.

III. IEEE 802.21 OVERVIEW

The present section shows the general architecture of the new IEEE 802.21 standard [2]. The standard specifies a Media Independent Handover (MIH) framework that facilitates handover in heterogeneous access networks (which may be wireless or wired) by exchanging information and defining commands and event triggers to assist in the handover decision making process.

The 802.21 standard supports cooperative use of information available at the MN and within the network infrastructure. Both the MN and the network may make decisions about connectivity in that the MN is well-placed to detect available networks and the network is suitable to store overall network information, such as neighborhood cell lists, location of MNs and higher layers of service availability.

To allow those functionalities, both the MN and the network PoA such as base stations and access points may be multi-modal (i.e., capable of supporting multiple radio standards and simultaneously allow connections on more than one radio interface). Specifically the standard consists of the

following elements:

- A framework that enables service continuity while a MN transitions between heterogeneous link-layer technologies.
- A set of handover-enabling functions within the protocol stacks of the network elements that provide the upper layers (e.g., mobility management protocols such as Mobile IP Mobile IPv6, Fast Mobile IP and SIP) with the required functionality to perform enhanced handovers. Usually, the upper layers protocols are referred as MIH users.
- A new logical entity created therein called the media independent handover function (MIHF). It is located in both local MN and the remote network node.
- A media independent handover service access point (named MIH_SAP) and associated primitives are defined to provide MIH users with access to the MIHF services.
- The definition of new link layer service access point and associated primitives for each link-layer technology. Moreover, IEEE 802.21 standard compatible equipment should be able to co-exist with legacy equipment.

The MIHF is the central entity of the emerging IEEE 802.21 standard (Fig.1). Its primary roles are to facilitate handovers and provide intelligence to the network selector entity. The MIHF also provides three primary services: event services, command services and information services. These services help the MIH users maintaining service continuity, quality of service monitoring, battery life conservation, network discovery and link selection. In the IEEE 802.21 terminology, these three services are generally referred to as mobility services (MoS). A detailed explanation of each mobility service follows.

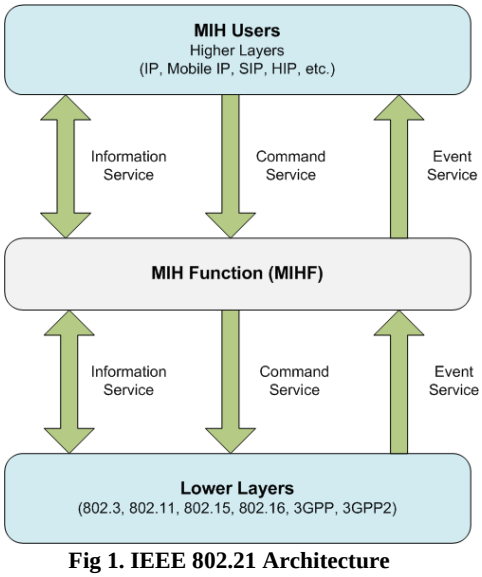

Fig 1. IEEE 802.21 Architecture

Media Independent Event Service

The media independent event service (MIES) is responsible for detecting events at lower layers and reporting them from both local and remote interfaces to the upper layers (the MIH users). A transport protocol is needed for supporting remote events. These events may indicate changes in state and transmission behavior of the physical, data link and logical link layers, or predict state changes of these layers.

Media Independent Command Service

The media independent command service (MICS) refers to the commands sent from MIH users to the lower (physical, data link, and logical link) layers in order to control it. The commands generally carry the upper layer decisions to the lower layers on the local device entity or at the remote entity. These commands are mandatory in nature and the recipient of a command is always expected to execute it.

MIH users may utilize command services to determine the status of links and/or control the multi-mode device for optimal performance. The MICS provides dynamic information such as signal strength and link speed, varying with time and MN mobility. The standard defines a number of commands to allow the MIH users to configure, control and retrieve information from the lower layers including MAC, radio resource management and physical layer.

Media Independent Information Service

The media independent information Service (MIIS) provides a framework and corresponding mechanisms by means of which a MIHF entity may discover and obtain network information existing within a geographical area to facilitate the handovers. MIIS includes support for various information elements which provide information that is essential for a network selector to make intelligent handover decisions. The information may be present in some MIIS server where the MIHF in the MN may access it.

Moreover, the MIIS provides capability for obtaining information about lower layers such as neighbor maps and other link layer parameters, as well as information about available higher layer services such as internet connectivity. For instance knowledge of whether security, supported channels, cost per use, networks categories (such as public, enterprise, home) and QoS supported may influence the decision to select such an access network during handover process. The MIIS also allows this collective information to be accessed from any single network. Information about a nearby Wi-Fi hotspot could be obtained using a Wi-Max interface or any cellular network, whether by means of request/response signaling without the need to power up the Wi-Fi interface. This capability allows the MN to use its currently active access network and inquire about other available access networks in a geographical region.

IV. MOBILITY INFORMATION STRUCTURE

The following section aims at describing the mobility information structure that can be used in heterogeneous wireless networks environment. At first, the IEEE 802.21 information elements and its categories are presented. Finally, we furnish a representative mobility information structure example describing its common data representation.

Information Elements (IEs)

As already mentioned, the MIIS provides a set of IEs (Fig.2) which offer link layer information parameters assisting the network selection algorithm to make intelligent handover decisions. Typically, the information supplied by these elements is intended to be static such as channel information, geographic position and security, although dynamic information must also be accounted for [4].

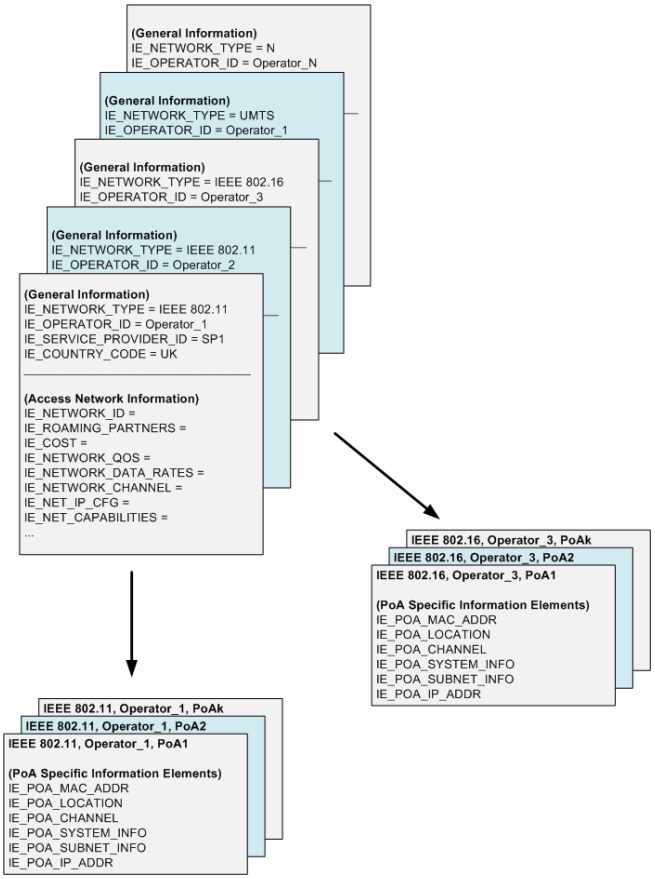

Fig 2. Mobility Information Structure

According with the IEEE 802.21 MIIS specification, the IEs can be divided in the following groups:

- General and access network information: give a general overview of the different available networks. These IEs are related to network type, operator, roaming agreements, cost per use or per traffic, security characteristics, QoS, data rate and type of mobility management protocol supported.
- Point of attachment (PoA) specific information: provides information about different PoAs for each available technology and operator. It covers information as MAC address of the PoA, IP configuration methods, channel range and geographical location.
- Vendor/network information: the standard can support other information such as access network specific, vendor/network proprietary services, etc.

The specification of IEs may involve both business and technical considerations. With regards to the business considerations, the main focus is on the Service Level Agreements (SLA) and possible charging rates that can or will be used in addition to the determination of specifically what IEs will be available. As an example, we may introduce the following use case: a MN detects two available wireless networks belonging to different operators. An operator may not want to disclose competitor´s information because this may lead MN moving out to the competition. In the case where one operator only reveals its own network information, a big problem arises as this could cause MN to not receive complete network´s information which could lead into a wrong handover decision. Referring to the technical issues, the IEs specification involves design, provisioning, discovery mechanisms, content delivery, transport-layer issues and security aspects.

Fig.2 shows a mobility information structure as specified in the IEEE 802.21 standard. It shows the IEs layout of different networks in a geographical area stored on a MIIS server. All the network information may be either centrally stored on a MIIS server or distributed in each of the individual access networks. A detailed explanation of MIIS server location as well as technical discussion can be found later.

In this example, the mobility information structure is composed by one MIIS server that stores information from three different operators named Operator_1, Operator_ 2 and Operator_3. According to the IEEE 802.21 MIIS specification, each information element is of IE_XXX form, where IE denotes information element and XXX denotes its description (i.e. IE_COST indicates the cost for service or network usage, IE_QOS indicates the QoS characteristics of the link layer, IE_POA_LOCATION indicates the geographical location of PoA and so on). The IEs are defined in a tree hierarchy representation in according with the three groups specified above.

As it can be seen in Fig.2, an operator can provide support for multiple access networks technologies. The first set of IEs is well-known as “General information” which gives a general overview of the different available networks. In this example, the Operator_1 supports both Wi-Fi and UMTS wireless networks. In addition, the Operator_2 holds up Wi-Fi and Wi-Max access networks. Finally, in the Operator_3 we can find out information from Wi-Max and UMTS networks. Under those circumstances, multiple operators can provide support for a particular network and a single network may support various access networks.

Likewise, for each network supported by an operator there is a set of IEs identified as “Access network information”. In this group of IEs, we can distinguish information such as cost per use, type of mobility management protocol supported, QoS characteristics, roaming partners, supported data rates, IP configuration methods among others.

Following the MIIS structure illustrated in Fig.2, the last set of IEs is defined as “PoA information” wherein each access network supply a list of supported PoAs. Thereby, the access network UMTS belonging to Operator_1 supports several

PoAs and the Wi-Max network from Operator_2 provides access to several PoAs as well. Here, we highlight important information such as the geographical location of PoA, its link layer and IP address, channel parameters and subnets supported. In summary, the MIIS structure offers mobility information that helps the MN to make an accurate handover decision across heterogeneous networks.

V. MIIS SIGNALING FLOW

In a heterogeneous wireless environment composed of several access networks, operators and MIIS servers, a series of steps are required before information is ready to be delivered back to MN when it is communicating with an MIIS server. In order to allow a MN to obtain network information, the deployment of an MIIS infrastructure would need to provide MIIS server discovery, integration of 802.21 networks with the IP transport layer and security association service in a variety of scenarios. The IETF MIPSHOP WG specified a general mobility framework design [5] for the IEEE 802.21 MIH protocol that addresses issues associated with the transport of MIH messages, services discovery mechanisms and security issues.

Fig.3 illustrates how a MN can obtain information from a MIIS server. The operation signaling flow between a MN and an MIIS server could be divided into the three following phases: discovery, security and transport.

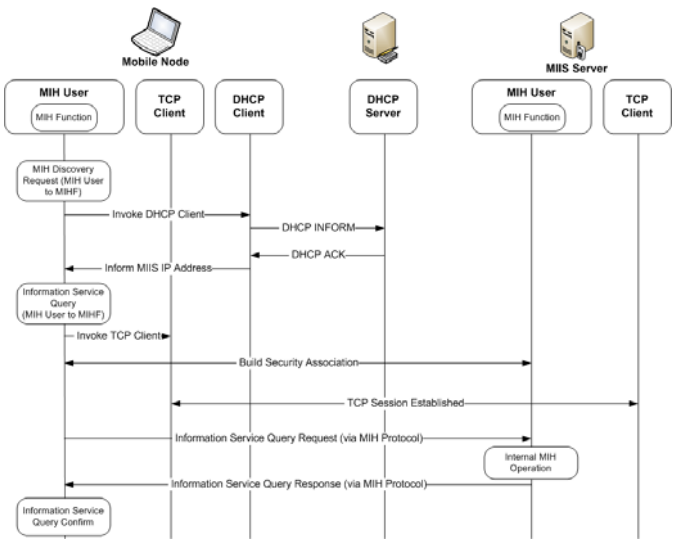

Fig 3. MN – MIIS Server Signaling Flow

The initial requirement is to provide the MN with a service discovery mechanism. In this way, the MN may use DHCP and DNS protocols for peer discovery which can operate over more than one network-layer hop. On the subject of the second requirement, a common security association method should be implemented between MN and MIIS server. Speaking about transport issues, the MN may use services provided by TCP and UDP for transporting 802.21 MIH messages which is not bound by any specific link layer technology. In this way, Fig.3 shows a MN requesting network information from a MIIS server. In this example, we use DHCP for MIIS server discovery and TCP for transport of MIH information. Following a detailed explanation of these three phases and interchanged messages is presented.

MIIS Server Discovery

The MIIS server discovery mainly depends on the MIIS server position in the network which may be one of the three scenarios described in [3]. The main objective of this first phase is to provide the MN with the IP address of the MIIS server. Efforts are currently underway to specify two discovery techniques: DNS and DHCP mechanisms. For a detailed operation of these service discovery mechanisms, see [6] and [7] respectively.

In the considered flow in Fig.3, we are using DHCP for MIIS server discovery. In order to obtain an IP address from the MIIS server, the MN´s DHCP client sends a DHCP Inform message according to standard DHCP but with a new DHCPv4 option called MoS options which allows the MN to locate a MIIS server which hosts the mobility services (MIES, MICS and MIIS). The document [7] also defines DHCPv6 options for mobility services discovery. Following the signaling flow, the DHCP server of MN´s network sends to the MN a DHCP Ack message containing the IP address of the MIIS server.

Security Aspects

The main objective of the MN using the MIIS information is to make an accurate handover decision. Thus, it is essential that the information comes from a reliable source. This requirement is even more imperative when handovers are done across IP subnets or administrative domains. In this sense, before exchanging information with a MIIS server, it may require a security association of the MN to provide access to certain information. It is important to note that in some scenarios the security association is not mandatory and the MIIS server may not require any authorization of the MN.

To ensure the validity of data communication between a MN and MIIS server, the IETF MOBOPTS WG is specifying a new secure handover optimization mechanism named media-independent pre-authentication (MPA) framework [11] that works over any link-layer and with any mobility management protocol including Mobile IPv4, Mobile IPv6, MOBIKE, HIP and SIP mobility.

In summary, MPA works assuming a MN which has connectivity to the current network but is not yet attached to any candidate network (CN). It´s functionality can be divided in four phases: (1) MN establishes a security association with the CN; (2) MN executes a configuration protocol to obtain an IP address as well as tunnel management protocol to establish a secure handover tunnel with the corresponding CN; (3) MN must send and receive packets over this secure handover tunnel; (4) the handover tunnel must be disabled immediately after the MN has attached to the CN.

Finally, the MPA framework can perform pre-authentication to establish the security mechanisms without assuming a common source of trust. This is very useful when

working over multiple operators without roaming agreement relationship. In this way, a security mobility association may works only based on a trust relationship between a MN and each administrative domain.

Transport Considerations

Once the IP address of the desired MIIS server has been discovered and a security association and connection is established, the MN and the IS server may exchange information over any supported transport protocol. The reference [9] is the main contribution to transport 802.21 MIH messages. It provides a container capability to mobility support services, as well as any required transport operation required to provide communication. Also, it discusses some particular mobility services characteristics as network loss, congestion conditions, message rate and retransmission parameters. As was previously stated, the MIIS framework provides the ability to access information about all networks in a geographical area from any single L2 or L3 networks depending on how the IS server is implemented.

Following the signaling flow in Fig.3, MN uses TCP protocol to establish a transport connection with the corresponding MIIS server. After established such connection, the MN may obtain network information sending a MIH_Get_Information message to the MIIS server. Once the MIIS server receives the MN´s query, it generates an appropriate response frame containing the necessary information to the MN.

After making the discovery procedure, a security association and the connection establishment, the MN has/receives all neighbor networks information and now it can take the handover decision. Detailed signaling flow inter-domain handover examples could be founded in [10] and [11].

VI. IMPLEMENTATION ISSUES

Several IEEE 802.21 simulations and implementations models were appeared in the last years, but it will consider the most important here. The first “implementation” was provided by NIST [12]. They developed NS-2 models of IEEE 802.21 MIH architecture components such as the Event, Command, and Information Services, and transport of Layer 2 trigger information to higher layers. They also produced a set of NS-2 models of MAC-layers such as IEEE 802.16 and IEEE 802.11 that are used with the MIH functions to model vertical, i.e. heterogeneous, handovers that are assisted by cross-layer information passage.

ODTONE [13] stands for Open Dot Twenty ONE and is an Open Source implementation of the Media Independent Handover standard using C++ APIs. ODTONE supplies the implementation of a MIHF, supporting its inherent MIES, MICS and MIIS, as well as supporting mechanisms (Capability Discovery, MIHF Registration, Event Registration, etc.). ODTONE aims to implement a MIHF that is capable of being deployed in multiple operating systems. In a first stage, it supports GNU/Linux, followed by Microsoft NT-based operating systems and others. This means this implementation will be decoupled of highly dependent operating system mechanisms.

VII. CONCLUSION

In this article we have discussed the main characteristics and features for the design of an information server infrastructure in heterogeneous wireless networks. The main benefit of using a MIIS framework is to enable the MN to gain an overview of their environment enabling it to make an accurate handover decision. We presented that there are several requirements that have to be considered when designing a generalized information server environment.

However, there are still some open issues that should be studied in future researches. Open investigation topics include new security mechanisms as new deployment real implementations modules.

ACKNOWLEDGMENTS

This work was supported by the Ministerio de Industria, Turismo y Comercio (MITyC, Spain) through the Project Avanza Competitividad I+D+I TSI-020100-2010-482 and the Ministerio de Ciencia e Innovación (MICINN, Spain) through the Project TEC2010-18894/TCM.

REFERENCES

[1] J. Manner and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[2] IEEE 802.21 Standard, “Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services”, January 2009.

[3] Fábio Buiati, Luis Javier García Villalba, Daniel Corujo, João Soares, Susana Sargento, Rui L. Aguiar, "Hierarchical Neighbor Discovery Scheme for Handover Optimization" IEEE Communication Letters, Vol.14, No.11, pp.1020-1022, November 2010.

[4] Y. Kim, S. Pack, C.G. Kang and S. Park, “An Enhanced Information Server for Seamless Vertical Handover in IEEE 802.21 MIH Networks”, Computer Networks, Vol. 55 (1), pp. 147-158, 2011.

[5] T Melia et al, "IEEE 802.21 Mobility Services Framework Design (MSFD) ", RFC 5677, December 2009.

[6] G. Bajko, "Locating IEEE 802.21 Mobility Services Using DNS”, RFC 5679, December 2009.

[7] G. Bajko and S. Das, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for IEEE 802.21 Mobility Services (MoS) Discovery”, RFC 5678, December 2009.

[8] A. Dutta, (Ed.), Y. Yohba, V. Fajardo, K. Taniuchi & H. Schulzrinneh, “A Framework of Media Independent Pre-Authentication (MPA) for Inter-Domain Handover Optimization”, draft-irtf-mobopts-mpa-framework-08.txt, September 2010, (work in progress).

[9] T. Melia, (Ed.), “RFC 5164 - Mobility Services Transport: Problem Statement”, March 2008.

[10] G. Lampropoulos, A. Salkintzis and N. Passas, "Media-Independent Handover for Seamless Service Provision in Heterogeneous Networks", IEEE Communications Magazine, Vol. 46 (1), pp. 64-71, January 2008.

[11] A. Oliva, A. Banchs, I. Soto, T. Melia and A.Vidal, “An Overview of IEEE 802.21: Media-Independent Handover Services”, IEEE Wireless Communications, Vol. 15 (4), pp. 96-103, August 2008.

[12] NIST Mobility Package for Network Simulator-2, May 2007.

[13] Odtone Open Dot Twenty ONE, http://hng.av.it.pt/projects/odtone.

Title: Overview of IEEE 802.21 Security Issues for MIH Networks

Author(s) name(s): Ismail Saadat, Fábio Buiati, Delfín Rupérez Cañas, Luis Javier García Villalba

Affiliation: Universidad Complutense de Madrid (UCM), Spain

Postal address:
Grupo de Análisis, Seguridad y Sistemas (GASS)
Departamento de Ingeniería del Software e Inteligencia Artificial (DISIA)
Facultad de Informática, Despacho 431
Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n
Ciudad Universitaria, 28040 Madrid, Spain

Phone number: +34 91.394.76.38

Fax number: +34 91.394.75.47

E-mail(s): {saadat, fabio, delfinrc, javiergv}@fdi.ucm.es

URL: http://gass.ucm.es/en/

Topic of the paper: Computer Networks & Communications

Title: Overview of IEEE 802.21 Security Issues for MIH Networks

Abstract: The convergence of different but complementary wireless networks brings the mobile user the opportunity to choose the network under an Always Best Connected scheme. In this heterogeneous environment the user can move between different administrative domains, aiming to make an inter-domain handover in a seamless manner. The IEEE 802.21 standard specifies a network information server entity providing network information within a geographical area by which the user can discover a service or a network. It is essential that the information comes from a reliable source. In this article, we describe the main technical requirements in order to establish a secure channel between the user and the information server. We also specify a scenario in which a proactive authentication mechanism is performed through an authentication server, focusing on optimization of the handover process.

***Index Terms* — Mobility, MPA, IEEE 802.21, Heterogeneous Networks, Inter-Domain, Security.**

Overview of IEEE 802.21 Security Issues for MIH Networks

Ismail Saadat, Fábio Buiati, Delfín Rupérez Cañas, Luis Javier García Villalba

***Abstract* - The convergence of different but complementary wireless networks brings the mobile user the opportunity to choose the network under an Always Best Connected scheme. In this heterogeneous environment the user can move between different administrative domains, aiming to make an inter-domain handover in a seamless manner. The IEEE 802.21 standard specifies a network information server entity providing network information within a geographical area by which the user can discover a service or a network. It is essential that the information comes from a reliable source. In this article, we describe the main technical requirements in order to establish a secure channel between the user and the information server. We also specify a scenario in which a proactive authentication mechanism is performed through an authentication server, focusing on optimization of the handover process.**

***Index Terms* — Mobility, MPA, IEEE 802.21, Heterogeneous Networks, Inter-Domain, Security.**

I. INTRODUCTION

THE significant increase of usage wireless networks such as Wi-Fi, Wi-Max and 3G, brings the mobile user the ability to make handovers under an Always Best Connected [1] scheme. In general, the handover process is divided into three main phases [2]: system discovery, handover decision and handover execution.

In the system discovery phase, the most important requirement is to provide the Mobile Node (MN) with sufficient information about neighbor networks to make an accurate handover decision. In the second phase, the user should choose a network based on several parameters such as quality of service (QoS), receive signal strength, access point geographical location, security mechanisms and so on. Finally, in the handover execution phase the connection is routed to the new access point in a seamless way.

In the literature [3] [4], the neighbor information discovery is the most time-consuming phase in the handover process. In this way, the network information discovery phase is highly critical. To accomplish it, the MN can consult a network information server, which can store information from several networks and operators. The IEEE 802.21 standard [5] specifies a media independent information service (MIIS) providing network information within a geographical area by which the user can discover a service or a network. However, it is essential that the information comes from a reliable source. This requirement is even more imperative when handovers are done across different administrative domains. Accessing critical information from other operator through non-secure links, and 3rd party servers, raises important security risk as well.

The MIIS needs both to protect itself from attack and provide MN provable trust, in order that they can exchange the information securely and make their handovers decisions without fear of malicious inaccuracies or mischief.

One solution in secure inter-domain handover is presented in [6]. The authors propose a Media-Independent Pre-Authentication (MPA) which is a mobile-assisted higher-layer authentication, authorization and handover scheme that is performed prior to establishing L2 connectivity to a network where mobile may move in near future. Using such a technique, the MN can establish a secure channel with the information server, performing a security communication.

The rest of this article is organized as follows. Initially, we briefly present the main entities and services of the emerging IEEE 802.21 standard are showed focusing on the information server domain as well as the related work on the security subject. Then we introduce the MPA protocol structure, including its elements and the communication process. Subsequently, we present a realistic scenario in which the MN performs an inter-domain handover obtaining the network information from a secure information server using the MPA protocol. As a final point, we conclude this work with some final considerations and open topics for future works.

II. IEEE 802.21 BACKGROUND AND RELATED WORK

A) IEEE 802.21 Background

The IEEE 802.21 standard [5] specifies a Media Independent Handover (MIH) framework that facilitates handover in heterogeneous access networks by exchanging information and defining commands and event triggers to assist in the handover decision making process. Specifically the standard consists of a framework that enables service continuity while a MN transitions between heterogeneous link-layer technologies. Also, it defines a new logical entity created therein called the media independent handover function (MIHF).

The MIHF is the central entity of the emerging IEEE 802.21 standard, as illustrated in Fig.1. Its primary roles are to facilitate handovers and provide intelligence to the network selector entity.

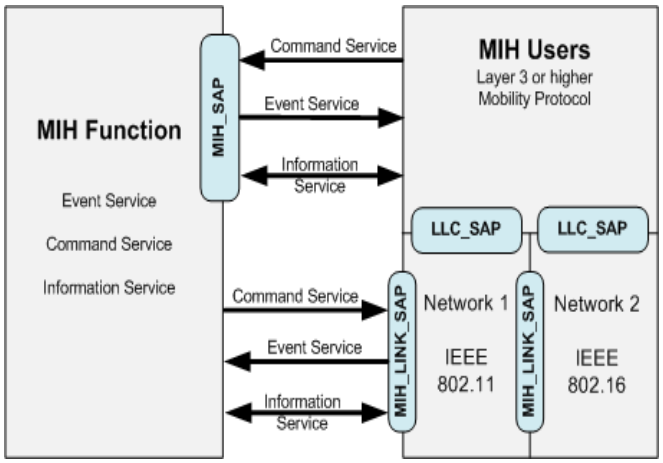

Fig. 1 - MIH Architecture Overview

The MIHF also provides three primary services: event services, command services and information services. These services help the MIH users maintaining service continuity, quality of service monitoring, battery life conservation, and network discovery and link selection. A detailed explanation of each mobility service follows.

The **media independent event service (MIES)** is responsible for detecting events at lower layers and reporting them from both local and remote interfaces to the upper layers (the MIH users). A transport protocol is needed for supporting remote events. These events may indicate changes in state and transmission behavior of the physical, data link and logical link layers, or predict state changes of these layers.

The **media independent command service (MICS)** refers to the commands sent from MIH users to the lower (physical, data link, and logical link) layers in order to control it. The commands generally carry the upper layer decisions to the lower layers on the local device entity or at the remote entity. MIH users may utilize command services to determine the status of links and/or control the multi-mode device for optimal performance.

The **media independent information Service (MIIS)** provides a framework and corresponding mechanisms by means of which a MIHF entity may discover and obtain network information existing within a geographical area to facilitate the handovers. MIIS includes support for various information elements which provide information that is essential for a network selector to make intelligent handover decisions. The information may be present in some MIIS server where the MIHF in the MN may access it. Moreover, the MIIS provides capability for obtaining information about lower layers such as neighbor maps and other link layer parameters, as well as information about available higher layer services such as internet connectivity. For instance knowledge of whether security, supported channels, cost per use, networks categories (such as public, enterprise, home) and QoS supported may influence the decision to select such an access network during handover process.

The information supplied by the MIIS is provided in Information Elements (IE) which can relate to higher layer services such as availability of IP mobility schemes at a certain operator, or to lower layer such as link neighbor maps and link configuration parameters (as illustrated in Fig.2). More concretely, information available via the MIIS can be categorized as:

• General and Access Network Specific Information: general overview of different networks, providing coverage within a specific area such as network type, operator and service identifier. Information including QoS, security, technology revision and cost is also available.

• Link connection point information: information about points of attachment for each access network available, comprising aspects such as MAC address of the access point, geographical location, channel configuration, and so on.

• Other information: network, service or vendor specific information.

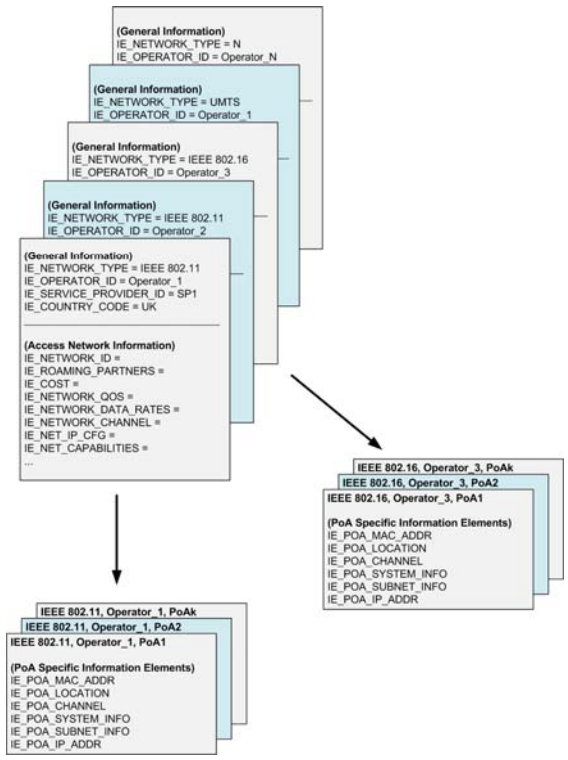

Fig. 2 – MIIS Information Elements

Detailed information about the IEEE 802.21 standard, its services and characteristics can be found in [7] and [8].

B) Related Work

The research community has been very active in recent years in reducing the disruptive effects of network handovers by proposing optimizations to existing mechanisms that add to existing mechanisms and external services and protocols that the help the transition from one network to another. However, there are few security mechanisms for MIH services in the literature.

To ensure the validity of data communication between a MN and MIIS server or any MIH entity, the IETF MOBOPTS WG[1] is specifying a new secure handover optimization mechanism denoted media-independent pre-authentication (MPA) framework [6][7] that works over any link-layer and with any mobility management protocol including Mobile IPv4, Mobile IPv6, MOBIKE, HIP and SIP mobility. The same authors are working in the IEEE 802.21a task group, the security extension to the existing IEEE 802.21 standard.

In [10], the authors present a flexible architecture which can efficiently handle the secure and seamless mobility issue in Wi-Fi / Wi-Max integrated networks deployed for enterprise system, completing most parts of authentication and key exchange process at the stage of initialization and handover procedure.

A new security scheme is presented by authors in [11]. They propose an efficient handover mechanism among Wi-Fi and Wi-Max networks which allows a seamless roaming process by reducing the authentication processes. This scheme also involves security mechanisms that guarantee the handover messages to be secure and maintain the authenticity. The authors still need to simulate the proposed scheme. The simulation will focus on time spent during authentication phase.

The authors in [12] propose a novel scheme to transport 802.21 messages over a secure network layer protocol denoted PLA that has built in hop-by-hop security mechanism. This scheme has the advantage that ensures very strong security of the signaling framework without much overhead. PLA-MIH reduces the latency during the MIH signaling. On the other hand, this work is only theoretical and the authors intend to do a detailed simulation scenario in future.

In [13], proactive authentication techniques and MIH protocol level security mechanisms are elaborated. Proactive authentication is a process by which an entity can perform a-priori network access authentication with a media independent authenticator and key holder (MIA-KH) that is serving a candidate network. The entity performs such authentication in anticipation of handover to the neighboring networks.

In [14] the authors propose an access authentication scheme with user anonymity denoted Secure Access of MIIS (SAM). The scheme provides an anonymous access authentication of MIIS considering that the access control for information is applied through an access authentication controller. The protocol can be used to establish a secure channel between the mobile node and the information server. The solution has the advantages of lightweight computation, low communication cost, and easy implementation, but it could have the disadvantage in a MIIS hierarchical framework.

In [15], Won et al propose a secure message transport (MIHSec) using the Master Shared Key (MSK) in order to overcome the handover overhead and hence minimizes authentication time. The MIHSec operates at the application layer and utilizes Extensible Authentication Protocol (EAP) to provide security to MIH messages.

In [16] the authors use the information capabilities provided by IEEE 802.21 and propose an extension to current network selection algorithms that takes into account security parameters and policies to optimize the handover performance and reduce the negotiation delay. The authors present two modular extensions to network selection algorithms that prevent the problems resulting from incompatible security policies, and provide more accurate security signaling delay estimations, which, in turn, result in more accurate handover delay estimations.

III. MEDIA PRE-AUTHENTICATION PROTOCOL (MPA)

The MPA [9] is a mobile-assisted higher-layer authentication, authorization and handover scheme that is performed prior to establishing link-layer connectivity to a network in which a MN may move in near future. As mentioned before, the MPA mobility optimization works with any mobility management protocol. With MPA, a MN can set parameters for Candidate Target Network (CTN) and also able to send and receive IP packets using the IP address obtained before it actually attaches to the CTN. Fig. 3 shows the main MPA functional components.

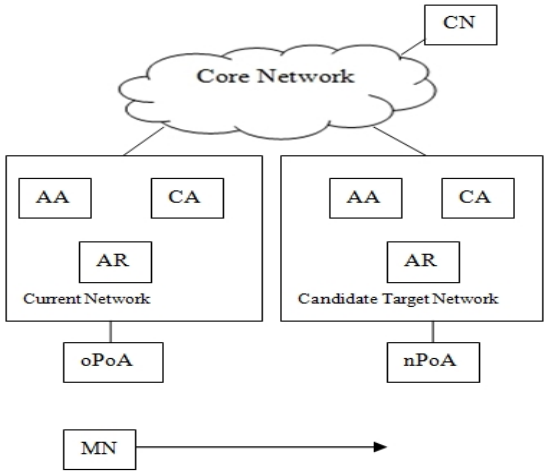

Fig. 3 - MPA Functional Components

In the MPA framework, the following functional elements are expected to reside in each CTN to communicate with a MN:

Authentication Agent (AA): it is responsible for the pre-authentication phase. An authentication protocol is executed between the MN and the authentication agent to establish an MPA-SA (MPA Secure Association). The authentication protocol should can to interact with an AAA entity such as Radius and Diameter to carry authentication credentials to an appropriate authentication server in the AAA infrastructure. The EAP (Extensible Authentication Protocol) [17] or ERP (EAP Reauthentication Protocol) [18] can be used as the authentication protocol for MPA.

Configuration Agent (CA): it is responsible for one part of

[1] IP Mobility Optimizations (Mob Opts) Research Group. The research group addresses questions of an evolutionary nature, starting with the current Mobile IP architecture, including handover optimizations such as Fast Handover and Hierarchical Mobile IP.

the pre-configuration phase, namely securely executing a configuration protocol to deliver an IP address and other configuration parameters to the MN. DHCP is an example of a configuration protocol that can be used to the configuration process.

Access Router (AR): it is a router that is responsible for the other part of pre-configuration process.

MPA Protocol Flow

In the MPA protocol flow, illustrated in Fig. 4, we assume that the MN is already connected to a point of attachment referred to as the old point of attachment (oPoA) and assigned an old CoA (oCoA). Next we explain each phase of the MPA process:

Stage 1: Pre-Authentication: The MN finds a CTN through a discovery process, and obtains the address and capabilities of the AA, CA, and AR in the CTN. The MN pre-authenticates with the authentication agent. If the pre-authentication is successful, an MPA-SA is created between the MN and the authentication agent. Two keys are derived from the MPA-SA, a MN-CA and MN-AR keys, which are used to protect subsequent signaling messages of a configuration protocol and a tunnel management protocol, respectively. The MN-CA and MN-AR keys are then securely delivered to the configuration agent and access router. Layer 2 pre-authentication is initiated at this stage.

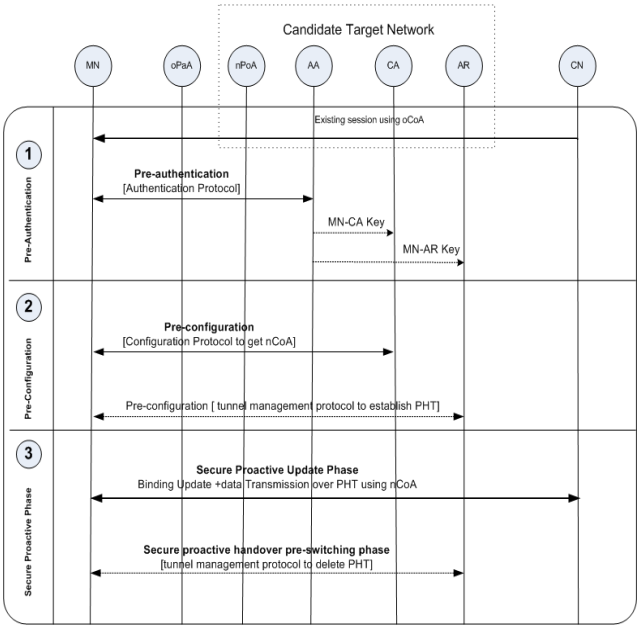

Fig 4 - MPA Phases

Stage 2: Pre-configuration: The MN realizes that its point of attachment is likely to change from oPoA to a new one, denoted new point of attachment (nPoA). Then it performs pre-configuration with the configuration agent to obtain several configuration parameters and default router from the CTN. The MN then communicates with the access router using the tunnel management protocol. A configuration protocol and a tunnel management protocol may be combined in a single protocol or executed in different orders depending on the actual protocol(s) used for configuration and tunnel management.

After completion of the tunnel establishment, the MN can communicate using both old *care-of address* (oCoA) and new *care-of address* (nCoA) by the end of step 3.

Stage 3: Secure proactive handover: The MN decides to switch to the nPoA. Before it switches to the nPoA, it starts a secure proactive handover by executing the binding update operation using a mobility management protocol and transmitting subsequent data traffic over the tunnel. This stage is divided into two minor phases:

Secure proactive handover pre-switching (sub-phase): The MN completes the binding update and becomes ready to switch to the new point of attachment. The MN might execute the tunnel management protocol to delete or disable the proactive handover tunnel and cache nCoA after deletion or disabling of the tunnel. This transient tunnel can be deleted prior to or after the handover. In this step, link-layer handover occurs.

Secure proactive handover post-switching (sub-phase): The MN executes the switching procedure. Upon successful completion of the switching procedure, the mobile node immediately restores the cached nCoA and assigns it to the physical interface attached to nPoA. If the proactive handover tunnel was not deleted or disabled, the tunnel is deleted or disabled as well. After this, direct transmission of data packets using nCoA is possible without using the tunnel.

MPA Applicability

The MPA can be used to optimize the mobility protocols that work in the network and application layers. The authors recommend that the MPA has more accuracy when the prediction of movement can be easily done. In other words, MPA is more viable as a solution for inter-domain predictive handover without the simultaneous use of multiple interfaces. Since MPA is not tied to a specific mobility protocol, it is also applicable to support optimization for inter-domain handover where each domain may be equipped with a different mobility protocol.

IV. PRACTICAL HANDOVER SCENARIO

This section presents a practical handover scenario that takes advantage of Wi-Fi and Wi-Max networks in which the MN get information from a secure IEEE 802.21 MIIS, as illustrated in the Fig. 5. We consider the MN as a multimodal device (equipped with two interfaces: Wi-Fi and Wi-Max). We assume that the MN is already connected to a point of attachment as the old point of attachment (oPoA) Wi-Max BS. The MIIS server is located in anywhere in the Internet. There is an AS (Authentication Server) that provides MIH level protection independent to media and access network.

Initially, the MN resides in Network1 and moves from its domain to another domain and in the process changes its subnet. Network 2 is the (nPoA) Wi-Fi AP, Network 3 is where the CN resides, and finally, Network 4 is where the MIIS server resides. Next we explain the signaling flow and how the MN obtains information from the MIIS in a secure manner.

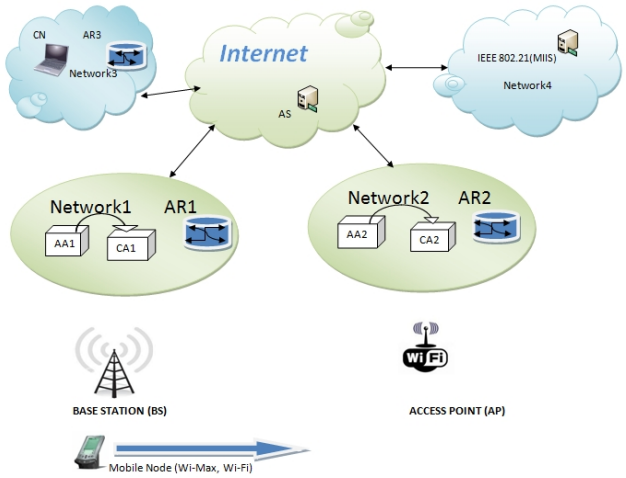

Fig. 5 - Integrated Wi-Fi and Wi-Max scenario

Fig. 6 depicts the handover signaling and mechanisms in an MPA scenario in which the MN is initially connected to the Wi-Max BS belonging to the Network1. We have divided the signaling into six minor phases, as follows:

At point 1, upon receiving a beacon from the Wi-Fi AP followed by a "*MIH_Link_Detected"* event from MAC layer toward the MIHF, the MN becomes aware of new connectivity opportunity. Discovery of neighboring networking elements such as access points, access routers, authentication servers helps expedite the handover process during a mobile's movement between networks.

At point 2, the MN first performs an authentication process with the AS server. Upon a successful authentication, a key is generated to the MIIS server (MN-MIIS). Then, the MN is authorized to ask the MIIS server for more information about the detected PoA. First, is sends a "*MIH_Get_Information request*" to the MIIS that answers with a "*MIH_Get_Information response*" message. In this phase, the MN also checks the resources availability at the candidate PoA (AP) and decides to make a handover. At the final, the MN obtains the IP addresses of AA2, CA2 AR2 from Network2.

At point 3, after the handover decision making, the MPA signaling starts (pre-authentication phase). The MN performs a pre-authentication with the authentication agent. If pre-authentication is successful, an MPA-SA is created between AA2 and MN. Two keys are derived from the MPA-SA, namely an MN-CA2 key and MN-AR2 key, which are used to protect subsequent signaling messages. The keys are then securely delivered to the CA2 and the AR2, respectively.

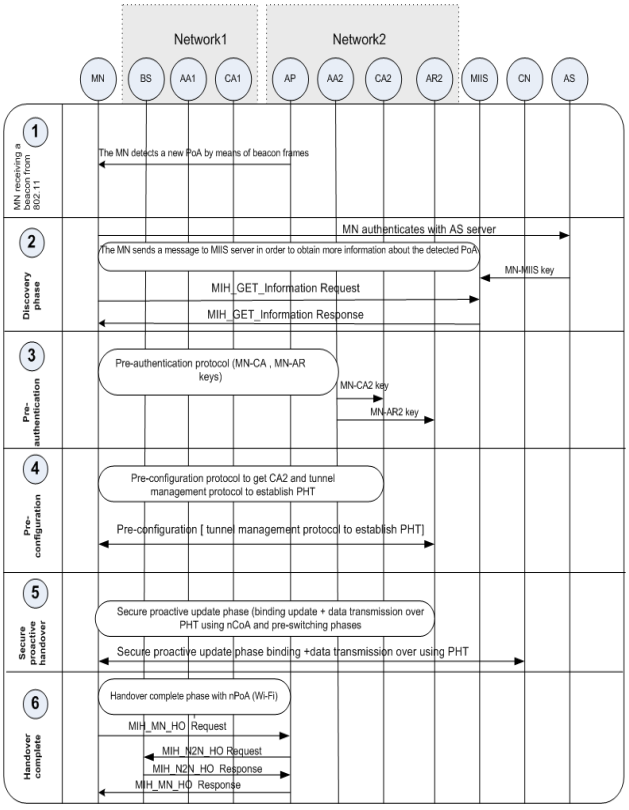

Fig. 6 – Handover signaling flow with a secure MIIS server.

At point 4, (pre-configuration phase), the MN realizes that its attachment is likely to change from Wi-Max (oPoA) to Wi-Fi (nPoA). It then performs a pre-configuration with CA2 using the configuration protocol to obtain several configuration parameters such as a new IP address and default router from Network2. The MN then starts a communication with the access router in Network2 using the tunnel management protocol to establish a proactive handover tunnel. The MN is able to communicate using both IP address from Network1 and IP address from Network2 by the end point 4. The signaling messages of the pre-configuration protocol are protected using the MN-CA2 key and the MN-AR2 key.

At point 5, (secure proactive handover), before the MN completes the binding update and becomes ready to switch to Wi-Fi, it starts secure proactive handover by executing the binding update operation of a mobility management protocol and transmitting data traffic over the tunnel. The MN may choose new addresses as the binding update address and send it to the CN. The MN completes the binding update and ready to switch to the Wi-Fi network. After that, the MN deletes or disables the proactive handover tunnel. The decision as to when the mobile node is ready to switch to the new point of attachment depends on the handover policy.

At Point 6, the MN finalizes the inter-domain handover by sending a "*MIH_MN _Handover_complete request*" message to the new PoA which confirms with the old PoA. Upon receiving the confirmation, the new PoA sends a "*MIH_MN _Handover_complete response*" message back to the MN.

Finally, the MN releases the allocated Wi-Max resources and deactivates the it´s corresponding interface.

V. CONCLUSION

In this article we have discussed the main characteristics and security issues in an inter-domain handover in heterogeneous wireless networks. We first described the MPA and its functional components. Then, through a practical scenario, we show an inter-domain signaling flow in which the MN can obtain information from a MIIS server in a secure manner.

As future work, we are working in a specification of new security mechanism as well as new deployment real implementations modules.

ACKNOWLEDGMENT

This work was supported by the Ministerio de Industria, Turismo y Comercio (MITyC, Spain) through the Project Avanza Competitividad I+D+I TSI-020100-2010-482 and the Ministerio de Ciencia e Innovación (MICINN, Spain) through the Project TEC2010-18894/TCM.

REFERENCES

[1] E. Gustafsson and A. Johnson, “Always Best Connected,” IEEE Wireless Communications, Vol. 10, No. 1, pp. 49-55, 2003.

[2] J. Manner and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[3] Sang-Jo Yoo, David Cypher and Nada Golmie, “Timely Effective Handover Mechanism in Heterogeneous Wireless Networks,” Proceedings of the Springer Wireless Personal Communications, 2008.

[4] J. Floroiu, M. Corici, Byoung-Joon Lee, S. Lee, S.Arbanowski, and T. Magedanz, “A Vertical Handover Architecture for End-to-End Service Optimization,” 16th IST Mobile and Wireless Communications Summit, 2007, July 2007.

[5] IEEE 802.21 Standard, “Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services”, January 2009.

[6] A. Dutta et al, “Media-Independent Pre-Authentication Supporting Secure Interdomain Handover Optimization”, IEEE Wireless Communications, Vol. 15, No. 2, pp. 55-64, April 2008.

[7] A. Oliva, A. Banchs, I. Soto, T. Melia and A.Vidal, “An Overview of IEEE 802.21: Media-Independent Handover Services”, IEEE Wireless Communications, Vol. 15 (4), pp. 96-103, August 2008.

[8] G. Lampropoulos, A. Salkintzis and N. Passas, "Media-Independent Handover for Seamless Service Provision in Heterogeneous Networks", IEEE Communications Magazine, Vol. 46 (1), pp. 64-71, January 2008.

[9] A. Dutta, (Ed.), Y. Yohba, V. Fajardo, K. Taniuchi & H. Schulzrinneh, “A Framework of Media Independent Pre-Authentication (MPA) for Inter-Domain Handover Optimization”, draft-irtf-mobopts-mpa-framework-08.txt, September 2010, (work in progress).

[10] J. Zhao, J. Pan and L. Hou, “Security and Seamless Mobility Based Architecture for Hybrid Network of Enterprise”, 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09, pp. 1, September 2009.

[11] H. Sun, S Chen, Y. Chen et al, “Secure and Efficient Handover Scheme for Heterogeneous Networks”, IEEE Asia-Pacific Services Computing Conference, 2008. APSCC '08, pp. 205, December 2008.

[12] S. Saha and D. Lagutin, “PLA-MIH: A Secure IEEE802.21 Signaling Scheme”, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009, pp. 252 – 257, November 2009.

[13] S. Das, A. Dutta, and T. Kodama, “Proactive authentication and MIH security,” 2009, https://mentor.ieee.org/802.21/documents.

[14] Guangsong Li, Qi Jiang, Xi Chen and Jianfeng Ma, “Secure Access Authentication for Media Independent Information Service”, EURASIP Journal on Wireless Communications and Networking, Volume 2010, Article ID 249169.

[15] J. Won, M. Vadapalli, C. Cho, and V. Leung, “Secure Media Independent Handover Message Transport in Heterogeneous Networks,” EURASIP Journal on Wireless Communications and Networking, Volume 2009, Article ID 716480.

[16] Antonio Izquierdo and Nada T. Golmie, “Improving Security Information Gathering with IEEE 802.21 to Optimize Handover Performance”, ACM. 2009.

[17] B. Aboba, D. Simon, and P. Eronen, “Extensible Authentication Protocol (EAP) Key Management Framework,” RFC 5247, 2008.

[18] V. Narayan and L. Dondeti, “EAP extensions for EAP re-authentication protocol (ERP),” RFC 5296, 2008.